C/2026/6013

17.11.2026

COMUNICAÇÃO DA COMISSÃO

Orientações da Comissão sobre a aplicação do Regulamento (UE) 2024/2847 (Regulamento de Ciber-Resiliência)

(C/2026/6013)

Índice

Página

1. INTRODUÇÃO 3
   - 1.1. Regulamento de Ciber-Resiliência 3
   - 1.2. Finalidade das orientações 3
2. ÂMBITO 4
   - 2.1. Colocação no mercado 4
   - 2.2. *Software* como produto com elementos digitais 5
   - 2.3. Código de computador 6
   - 2.4. Combinação de *hardware* e *software* que forma um produto com elementos digitais 7
   - 2.5. Conexão de dados 8
   - 2.6. Sistemas complexos 8
   - 2.7. Produtos com elementos digitais concebidos antes do início da aplicação do Regulamento de Ciber-Resiliência 9
3. *SOFTWARE* LIVRE E DE CÓDIGO-FONTE ABERTO 11
   - 3.1. Determinar se o *software* livre e de código-fonte aberto está sob a sua responsabilidade 12
   - 3.2. Determinar se o *software* livre e de código-fonte aberto é colocado no mercado da UE 13
     - 3.2.1. Cobrança de um preço 13
     - 3.2.2. Monetização de outros serviços ou exigência do tratamento de dados pessoais 13
     - 3.2.3. Serviços de apoio 14
     - 3.2.4. Donativos 15
     - 3.2.5. Financiamento do *software* livre e de código-fonte aberto 15
     - 3.2.6. Entidades sem fins lucrativos criadas para alcançar objetivos sem fins lucrativos 16
     - 3.2.7. Integração por outros fabricantes 16
   - 3.3. Administradores de *software* de código-fonte aberto 16
     - 3.3.1. Apoio contínuo e garantia da viabilidade do SL/A 17
   - 3.4. Contribuintes e utilizações a jusante 18
   - 3.5. Cenários ilustrativos 19
4. MODIFICAÇÕES SUBSTANCIAIS E PEÇAS SOBRESSELENTES 21
   - 4.1. Reparações físicas 22
   - 4.2. Peças sobresselentes 23
   - 4.3. Atualizações de *software* como modificações substanciais 24

4.4. Consequências de uma modificação substancial 27
4.4.1. Modificações substanciais efetuadas por outra pessoa que não o fabricante original 28
4.4.2. Modificações substanciais efetuadas pelo fabricante original 29
5. PERÍODO DE APOIO 29
5.1. Modificações substanciais e período de apoio 31
6. PRODUTOS IMPORTANTES E CRÍTICOS COM ELEMENTOS DIGITAIS 32
6.1. Funcionalidade principal 33
6.2. Avaliação da conformidade para produtos importantes e críticos com elementos digitais 36
6.3. Implicações para a presunção de conformidade 38
7. AVALIAÇÃO DOS RISCOS DE CIBERSEGURANÇA E INTEGRAÇÃO DE PRODUTOS COM ELEMENTOS DIGITAIS E COMPONENTES 41
7.1. Sobre a avaliação e o tratamento dos riscos de cibersegurança 41
7.2. Sobre a conceção, desenvolvimento e produção de produtos com elementos digitais de modo a garantir um nível adequado de cibersegurança com base nos riscos 42
7.3. Avaliação dos riscos e diligência devida em relação às dependências externas e aos componentes integrados 42
7.4. Reutilização de avaliações dos riscos e de documentação de conformidade para famílias de produtos com elementos digitais 44
8. TRATAMENTO REMOTO DE DADOS 44
8.1. O que se considera ser uma solução de tratamento remoto de dados para um produto com elementos digitais? 45
8.1.1. O conceito de «à distância» 46
8.1.2. A inexistência desse tratamento de dados impediria o produto com elementos digitais de desempenhar uma das suas funções? 46
8.1.3. O *software* foi concebido e desenvolvido pelo fabricante ou sob a sua responsabilidade? 47
8.2. Implicações práticas e técnicas das soluções de tratamento remoto de dados e recurso a soluções de terceiros 49
8.3. Casos de utilização para soluções de tratamento remoto de dados 50
8.3.1. Aplicação bancária móvel 51
8.3.2. Termóstato inteligente 52
8.3.3. Leitor de livros digitais 53
8.3.4. Robô industrial 53
8.3.5. Rede celular 53
9. ELEMENTOS ADICIONAIS 54
9.1. Obrigações em matéria de comunicação de informações 54
9.2. Tratamento de vulnerabilidades 56
9.2.1. Comunicação de informações a montante e partilha de correções de segurança 56
9.2.2. Vulnerabilidades passíveis de serem exploradas conhecidas 57
9.2.3. Ensaios e análises eficazes e regulares 58
9.3. Interação com outros atos legislativos 59
9.3.1. Regulamento (UE) 2019/2144 e Regulamento (UE) n.º 168/2013 59
9.3.2. Validade dos certificados de exame UE de tipo (artigo 69.º, n.º 1) 59

1. **INTRODUÇÃO**

1.1. **Regulamento de Ciber-Resiliência**

1. O 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) ([1]) entrou em vigor em 10 de dezembro de 2024. O regulamento visa reforçar a abordagem da UE à cibersegurança, incidir sobre a ciber-resiliência a nível da UE 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 UE, bem como durante o ciclo de vida de um produto com elementos digitais.

2. O Regulamento de Ciber-Resiliência baseia-se no novo quadro legislativo (NQL) da UE estabelecido no 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 fiscalização do mercado relativos à comercialização de produtos, e que revoga o Regulamento (CEE) n.º 339/93, e na 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 do Conselho ([2]).

3. A fiscalização do mercado e a aplicação da legislação são asseguradas pelas autoridades nacionais de fiscalização do mercado. Os produtos com elementos digitais que se enquadram no âmbito de aplicação do Regulamento de Ciber-Resiliência são abrangidos pelo 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. A Comissão e a Agência da União Europeia para a Cibersegurança (ENISA) apoiam os operadores económicos e os Estados-Membros na aplicação do Regulamento de Ciber-Resiliência.

1.2. **Finalidade das orientações**

4. O artigo 26.º, n.º 1, do Regulamento de Ciber-Resiliência exige que a Comissão publique orientações para ajudar os operadores económicos a aplicar o regulamento, dando especial destaque à facilitação do cumprimento por parte das microempresas e das pequenas e médias empresas (PME). O artigo 26.º, n.º 2, estabelece os aspetos mínimos que devem ser tidos em conta nas orientações. Inclui-se: i) o âmbito de aplicação do Regulamento de Ciber-Resiliência (em especial soluções de tratamento remoto de dados e *software* livre e de código-fonte aberto), ii) o conceito de «períodos de apoio», iii) a interação entre o Regulamento de Ciber-Resiliência e outra legislação da UE e iv) o conceito de «modificação substancial».

5. Em 3 de dezembro de 2025, a Comissão publicou uma série de perguntas frequentes, destinadas a ajudar os operadores económicos a prepararem-se para a aplicação do Regulamento de Ciber-Resiliência ([3]).

6. As presentes orientações destinam-se a ajudar os operadores económicos a cumprir o Regulamento de Ciber-Resiliência e a apoiar as atividades das autoridades de fiscalização do mercado, das autoridades notificadoras e dos organismos notificados, com vista a assegurar a aplicação harmonizada do Regulamento de Ciber-Resiliência em toda a União. Não pretendem abranger a totalidade do âmbito de aplicação do Regulamento de Ciber-Resiliência, mas sim prestar esclarecimentos sobre a fundamentação de determinadas disposições fundamentais e a forma como podem ser aplicadas na prática. As presentes orientações dizem respeito ao Regulamento de Ciber-Resiliência e não são aplicáveis a outros atos legislativos da UE.

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

([2]) O programa de trabalho da Comissão para 2026 prevê a apresentação de um «ato legislativo europeu sobre os produtos», que atualiza o NQL e as regras relativas à fiscalização do mercado e à normalização: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52025DC0870.

([3]) É possível descarregar as perguntas frequentes através do sítio Web de aplicação do Regulamento de Ciber-Resiliência da Comissão, a partir da página Web específica das perguntas frequentes.

7. Durante a elaboração das presentes orientações, as partes interessadas foram amplamente consultadas, inclusive no quadro do Grupo de Peritos em Cibersegurança de Produtos com Elementos Digitais ([4]) e através de uma consulta pública realizada entre 3 de março e 13 de abril de 2026 ([5]).

8. As presentes orientações não são vinculativas para os operadores económicos ou outros intervenientes sujeitos ao Regulamento de Ciber-Resiliência. Só o Tribunal de Justiça da União Europeia poderá apresentar uma interpretação vinculativa do Regulamento de Ciber-Resiliência. Todavia, as presentes orientações definem a interpretação que a Comissão faz do regulamento, com vista a apoiar o seu cumprimento e contribuir para a sua aplicação efetiva. Além disso, as orientações contêm uma série de exemplos para ilustrar a aplicação de disposições específicas. No entanto, estes exemplos não se destinam a substituir uma avaliação caso a caso, que será sempre necessária para ter em conta as especificidades de cada caso individual.

9. Em conformidade com o artigo 26.º do Regulamento de Ciber-Resiliência, a Comissão pode ponderar a emissão de orientações adicionais, incluindo orientações destinadas aos fabricantes sujeitos ao referido regulamento e a outra legislação de harmonização da União ou a outros atos jurídicos conexos da União. As presentes orientações podem, por exemplo, responder a questões sobre a interação entre o Regulamento de Ciber-Resiliência e o Regulamento (UE) 2024/1689 que cria regras harmonizadas em matéria de inteligência artificial (Regulamento IA), bem como com o Regulamento (UE) 2022/2554 relativo à resiliência operacional digital do setor financeiro (Regulamento DORA).

2. **ÂMBITO**

2.1. **Colocação no mercado**

10. O Regulamento de Ciber-Resiliência aplica-se aos produtos com elementos digitais disponibilizados no mercado da UE. O conceito de «disponibilização no mercado» é definido no artigo 3.º, ponto 22, do Regulamento de Ciber-Resiliência como «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». Em conformidade com o artigo 3.º, ponto 21, um produto com elementos digitais é colocado no mercado da UE aquando da primeira disponibilização.

11. A última edição do «Guia Azul sobre a aplicação das regras da UE em matéria de produtos», publicada em 2022 (a seguir designado por «Guia Azul») ([6]), faculta orientações que facilitam a compreensão das regras da UE em matéria de produtos e a sua aplicação uniforme nos diferentes quadros jurídicos setoriais alinhados com o novo quadro legislativo (NQL), como o Regulamento de Ciber-Resiliência. O Guia Azul indica que os conceitos de «colocação no mercado» e de «disponibilização» devem ser entendidos como referindo-se «a cada produto individual e não a um tipo de produto, independentemente de ter sido fabricado como uma unidade individual ou em série» (secção 2.3).

12. No caso dos produtos com elementos digitais mais «tradicionais» abrangidos pelo NQL, como *hardware* sob a forma de máquinas ou produtos de equipamentos de rádio com elementos digitais, o conceito de «colocação no mercado» está bem estabelecido e o Guia Azul faculta orientações adicionais para clarificar quando se considera que esses produtos são colocados no mercado. Os «breves exemplos» constantes da secção 2.12 do Guia Azul proporcionam mais exemplos do conceito de «colocação no mercado».

13. Todavia, dada a natureza dos produtos incorpóreos com elementos digitais, como o *software* autónomo, são necessárias orientações adicionais sobre quando se considera que esses produtos com elementos digitais são colocados no mercado. Quando a fase de fabrico do *software* está concluída e o produto com elementos digitais é oferecido a potenciais utilizadores no mercado da UE, pode considerar-se que o seu fabricante fabricou várias cópias do mesmo produto de *software* com elementos digitais e as forneceu para distribuição ou utilização. Com efeito, ao contrário dos produtos corpóreos com elementos digitais, o *software* autónomo não está sujeito a

([4]) Grupo de Peritos em Cibersegurança de Produtos com Elementos Digitais no registo dos grupos de peritos da Comissão e outras entidades semelhantes.
([5]) Consulta pública sobre o projeto de orientações da Comissão sobre o Regulamento de Ciber-Resiliência.
([6]) Comunicação da Comissão — Guia Azul de 2022 sobre a aplicação das regras da UE em matéria de produtos, 2022/C 247/01 (JO C 247 de 29.6.2022, p. 1).

limitações físicas de produção ou de existências: cada ato de disponibilização do *software* para descarregamento ou distribuição resulta na criação de uma nova cópia idêntica para o utilizador. Desde que esta versão do *software* não seja modificada de uma forma que afete o cumprimento do Regulamento de Ciber-Resiliência, considera-se que a colocação no mercado da UE ocorreu no momento da primeira oferta para distribuição ou utilização. Por conseguinte, deve considerar-se que a possibilidade de descarregar ou distribuir posteriormente esta versão do produto de *software* com elementos digitais constitui um caso em que este produto de *software* com elementos digitais é disponibilizado ([7]).

14. Por conseguinte, deve considerar-se que um produto de *software* autónomo com elementos digitais foi colocado no mercado quando a sua fase de fabrico estiver concluída e esse *software* for fornecido pela primeira vez para distribuição ou utilização no mercado da UE no âmbito de uma atividade comercial. Deverá considerar-se que o fabricante colocou no mercado várias cópias do mesmo produto de *software* com elementos digitais ao mesmo tempo. Assim, embora várias cópias do mesmo *software* continuem a ser produtos individuais com elementos digitais, considera-se que são colocadas no mercado ao mesmo tempo, independentemente do momento em que a posse ou a utilização de cada cópia individual é transferida para outra pessoa singular ou coletiva. Simultaneamente, se o fabricante disponibilizar *software* em diferentes variantes que diferem nos seus componentes, configurações ou funcionalidades ativadas incluídos (por exemplo, versões para diferentes sistemas operativos ou pacotes com conjuntos de características diferentes), essas variantes não podem ser consideradas cópias múltiplas do mesmo produto de *software* com elementos digitais. Por conseguinte, para efeitos de colocação no mercado, devem ser tratadas como produtos distintos com elementos digitais.

Exemplo 1: em 1 de janeiro de 2028, a empresa A disponibiliza pela primeira vez, através do seu sítio Web, a versão 1.0.0 do seu software *X. No mesmo dia, o cliente 1 compra uma cópia da versão 1.0.0 do* software *X. Em 15 de janeiro de 2028, o cliente 2 compra uma cópia da versão 1.0.0 do* software *X. Ambas as cópias da versão 1.0.0 do* software *X são colocadas no mercado em 1 de janeiro de 2028.*

15. Dada a natureza iterativa do desenvolvimento de *software*, importa clarificar ainda que se considera que as iterações subsequentes de um produto de *software* com elementos digitais foram recentemente colocadas no mercado quando essas iterações forem consideradas uma «modificação substancial» de um produto de *software* com elementos digitais já colocado no mercado, conforme indicado no considerando 41 do Regulamento de Ciber-Resiliência. As iterações que não sejam consideradas modificações substanciais não exigem que o fabricante realize um novo procedimento de avaliação da conformidade e, por conseguinte, não modificam a data de colocação desse *software* no mercado. Para mais orientações sobre o conceito de «modificações substanciais», ver a secção *4 Modificações substanciais.*

Exemplo 2: em 1 de janeiro de 2028, a empresa A disponibiliza pela primeira vez, através do seu sítio Web, a versão 1.0.0 do software *X. No mesmo dia, o cliente 1 adquire uma cópia da versão 1.0.0 do* software *X. Em 15 de janeiro de 2028, a empresa A lança uma versão 1.0.1 atualizada do* software *X que não constitui uma modificação substancial. Em 30 de janeiro de 2028, o cliente 2 compra uma cópia da versão 1.0.1 do* software *X. Considera-se que ambas as cópias das versões 1.0.0 e 1.0.1 do* software *X foram colocadas no mercado em 1 de janeiro de 2028.*

16. As orientações apresentadas nos pontos 13, 14 e 15 aplicam-se exclusivamente na medida em que o produto com elementos digitais seja *software* autónomo. Tal não é o caso, por exemplo, quando o *software* é combinado com *hardware*, conforme referido na secção *2.4 Combinação de hardware e software que forma um* produto.

2.2. ***Software* como produto com elementos digitais**

17. O artigo 3.º, ponto 1, do Regulamento de Ciber-Resiliência define «produto com elementos digitais» como «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». Esses produtos com elementos digitais enquadram-se no âmbito de aplicação do Regulamento de Ciber-Resiliência caso a sua finalidade prevista ou utilização razoavelmente previsível inclua uma conexão de dados lógica ou física, direta ou indireta, a um dispositivo ou a uma rede.

([7]) Nos termos do artigo 13.º, n.º 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.

18. Por conseguinte, o Regulamento de Ciber-Resiliência pode abranger uma série de produtos com elementos digitais, nomeadamente: i) *software* autónomo, como aplicações e programas informáticos, distribuído digital ou fisicamente, ii) *hardware* com *software* incorporado (por exemplo, dispositivos da Internet das coisas, computadores portáteis, tábletes), iii) *hardware* autónomo (por exemplo, circuitos integrados, placas-mãe) e iv) qualquer combinação de *hardware* e *software* fornecida separadamente, mas destinada a funcionar em conjunto.

19. Por conseguinte, o *software* autónomo é abrangido pelo âmbito de aplicação do Regulamento de Ciber-Resiliência quando é colocado no mercado como um produto com elementos digitais. Importa distinguir os produtos de *software* com elementos digitais que estão sujeitos ao Regulamento de Ciber-Resiliência e a prestação à distância de serviços que não são abrangidos pelo âmbito de aplicação desse regulamento.

20. Para que o *software* seja abrangido pelo âmbito de aplicação do Regulamento de Ciber-Resiliência, um produto de *software* com elementos digitais deve ser fornecido a um utilizador, obtido por esse utilizador e operado num sistema de informação eletrónico, ou como parte de um, do lado do utilizador. O *software* que é descarregado, instalado ou fornecido de outra forma ao utilizador e que é executado no sistema de informação eletrónico do utilizador cumpre estes critérios, incluindo, por exemplo, quando assume a forma de uma extensão de navegador ou de uma aplicação desenvolvida com tecnologias Web, mas fornecida para execução local.

21. Em contrapartida, um *software* que é executado à distância e ao qual o utilizador se limita a aceder não é, só por isso, um produto com elementos digitais. Com efeito, os considerandos 11 e 12 do Regulamento de Ciber-Resiliência estabelecem esta distinção, explicando que o tratamento ou o armazenamento à distância só estão sujeitos a este regulamento na medida em que seja necessário para que um produto com elementos digitais desempenhe as suas funções (ou seja, através do conceito de tratamento remoto de dados, conforme definido no artigo 3.º, ponto 2, e não como um produto com elementos digitais. É normalmente o caso das aplicações Web, incluindo as aplicações Web progressivas, caso se aceda exclusivamente através de um navegador Web. O mesmo se aplica aos sítios Web: embora estes possam, numa medida limitada, funcionar e ser executados tecnicamente no dispositivo do utilizador, decorre do considerando 12 do Regulamento de Ciber-Resiliência que os sítios Web não são, eles próprios, considerados produtos com elementos digitais e só são abrangidos pelo âmbito de aplicação desse regulamento se apoiarem a funcionalidade de um produto com elementos digitais, ou seja, na medida em que se qualifiquem como tratamento remoto de dados (conforme explicado mais pormenorizadamente na secção *8* e, especialmente, *8.1.2 A inexistência desse tratamento de dados impediria o produto com elementos digitais de desempenhar uma das suas funções?*).

Exemplo 3: uma aplicação móvel que um utilizador descarrega de uma loja de aplicações e instala no seu telemóvel inteligente é fornecida ao utilizador e executada no dispositivo deste, sendo, por conseguinte, um produto com elementos digitais. Quando é colocada no mercado no âmbito de uma atividade comercial, pode ser abrangida pelo âmbito de aplicação do Regulamento de Ciber-Resiliência.

Exemplo 4: uma aplicação para computador criada com recurso a tecnologias Web, mas colocada num pacote para instalação local, é fornecida ao utilizador e executada no dispositivo deste, sendo, por conseguinte, um produto com elementos digitais. Quando é colocada no mercado no âmbito de uma atividade comercial, pode ser abrangida pelo âmbito de aplicação do Regulamento de Ciber-Resiliência.

Exemplo 5: uma aplicação Web a que o utilizador acede exclusivamente através de um navegador Web não é um produto com elementos digitais. A menos que apoie a funcionalidade de um produto com elementos digitais, não é abrangida pelo âmbito de aplicação do Regulamento de Ciber-Resiliência. Em contrapartida, uma aplicação fornecida ao utilizador enquanto cliente instalado localmente e executada no dispositivo deste é um produto com elementos digitais. Quando é colocada no mercado no âmbito de uma atividade comercial, pode ser abrangida pelo âmbito de aplicação do Regulamento de Ciber-Resiliência.

Se, para desempenhar uma ou mais das suas funções, esse cliente recorrer a um tratamento de dados à distância que corresponda à definição de tratamento remoto de dados, esse tratamento de dados à distância também faz parte do produto com elementos digitais.

Exemplo 6: um sítio Web que se limite a apresentar informações aos seus visitantes e não apoie a funcionalidade de um produto com elementos digitais não é, ele próprio, um produto com elementos digitais. Por conseguinte, não é abrangido pelo âmbito de aplicação do Regulamento de Ciber-Resiliência.

2.3. **Código de computador**

22. É igualmente útil clarificar se o código-fonte pode constituir um produto de *software* com elementos digitais. O Regulamento de Ciber-Resiliência define «*software*» como «a parte de um sistema de informação eletrónico que consiste em código de computador» (artigo 3.º, ponto 4). O código de computador pode assumir a forma de i) código-máquina, que é o conjunto de instruções executadas diretamente pelo processador de um computador, escrito em formato binário, ou ii) código-fonte, ou seja, o conjunto de instruções e declarações redigidas numa linguagem de programação, que devem ser compiladas ou interpretadas para serem executadas por um computador. A definição de *software* constante do Regulamento de Ciber-Resiliência abrange ambas as formas.

23. Uma questão distinta consiste em saber se um determinado fornecimento de código de computador equivale a colocar um produto com elementos digitais no mercado da UE, o que exige um fornecimento no âmbito de uma atividade comercial. Muitas vezes, tal pode não ser o caso do código-fonte. Por exemplo, uma pessoa singular ou coletiva que partilhe código de computador livre e de código-fonte aberto em repositórios acessíveis ao público não é geralmente considerada como estando a colocar esse código no mercado da UE para efeitos do Regulamento de Ciber-Resiliência (conforme analisado mais pormenorizadamente na secção *3 Software livre e de* código-fonte aberto). O código inacabado partilhado durante a fase de conceção e desenvolvimento de um produto com elementos digitais (por exemplo, para ensaio ou revisão) também não é considerado colocado no mercado para efeitos do Regulamento de Ciber-Resiliência, pois a sua fase de fabrico não está concluída. Do mesmo modo, o código de amostragem ou de demonstração fornecido no âmbito de tutoriais ou materiais de formação também não é considerado colocado no mercado para efeitos do Regulamento de Ciber-Resiliência ([8]).

24. Por outro lado, quando um fabricante fornece aos seus clientes um código de computador como um produto com elementos digitais, considera-se que esse código foi colocado no mercado, independentemente de se tratar de código-máquina ou de código-fonte ([9]).

Exemplo 7: a empresa A licencia código-fonte à empresa B para uma plataforma interna personalizável e fornece esse código-fonte num ficheiro de texto. Mesmo que esse código-fonte exija adaptação e compilação adicionais por parte da empresa B antes de ser utilizado, a empresa A está a colocar esse código-fonte no mercado e, por conseguinte, está sujeita ao Regulamento de Ciber-Resiliência. A empresa A não é responsável pelo cumprimento do Regulamento de Ciber-Resiliência das subsequentes adaptações e compilação desse código por parte da empresa B.

2.4. **Combinação de *hardware* e *software* que forma um produto com elementos digitais**

25. A questão de saber se o *software* faz parte de um produto com elementos digitais não deve ser determinada pela forma ou pelo momento em que esse *software* é fornecido ao utilizador, mas sim pelo facto de, tendo em conta a finalidade prevista do produto e a sua utilização razoavelmente previsível, o *software* ser necessário para que o produto com elementos digitais desempenhe as funções previstas. Caso um produto de *hardware* com elementos digitais seja concebido para trabalhar em conjunto com um *software* específico fornecido pelo mesmo fabricante para desempenhar as suas funções, o *hardware* e esse *software*, em conjunto, constituem o produto com elementos digitais. Por conseguinte, o *software* necessário para operar, configurar, controlar ou utilizar um produto com elementos digitais em conformidade com a sua finalidade prevista faz parte do produto com elementos digitais, mesmo que seja obtido através de um canal separado (por exemplo, uma loja de aplicações, uma ligação de descarregamento ou outro canal digital após o produto de *hardware* com elementos digitais ter sido colocado no mercado). Por conseguinte, a sua colocação no mercado ocorre no mesmo momento em que as unidades dos produtos de *hardware* com elementos digitais são colocadas no mercado.

Exemplo 8: uma impressora em rede é colocada no mercado como um produto de hardware *com elementos digitais, ao passo que os controladores de* software *necessários para enviar trabalhos de impressão, configurar o dispositivo e gerir o seu funcionamento são disponibilizados para descarregamento a partir do sítio Web do fabricante. Embora a impressora e os controladores sejam fornecidos através de canais diferentes, constituem, em conjunto, um produto único com elementos digitais, pois a impressora não pode cumprir a sua finalidade prevista sem os controladores.*

Exemplo 9: um dispositivo usável de monitorização da condição física é colocado no mercado para medir a frequência cardíaca e a atividade de um utilizador, sendo necessária uma aplicação para telemóveis inteligentes fornecida pelo fabricante a fim de apresentar as medições, mostrar o historial e permitir a configuração do dispositivo. Embora a aplicação seja descarregada separadamente através de uma loja de aplicações, o dispositivo usável e a aplicação, em conjunto, constituem um produto único com elementos digitais, uma vez que são concebidos e destinados a funcionar em conjunto para proporcionar a funcionalidade do produto com elementos digitais.

([8]) Importa igualmente recordar que o artigo 4.º, n.º 3, permite que os fabricantes disponibilizem no mercado *software* inacabado que não cumpra o disposto no regulamento, como versões alfa, versões beta ou candidatos a lançamento, contanto que o *software* inacabado só seja disponibilizado durante o tempo necessário para testá-lo e recolher opiniões.

([9]) Por outro lado, importa salientar que, para efeitos da legislação sobre a responsabilidade dos produtos, o próprio código de computador não constitui um produto e, por conseguinte, os fabricantes que colocam esse código no mercado não podem ser responsabilizados nos termos da Diretiva (UE) 2024/2853 (Diretiva Responsabilidade dos Produtos). O considerando 13 da referida diretiva enuncia que «[c]ontudo, a informação não deve ser considerada um produto e as regras em matéria de responsabilidade decorrente dos produtos não deverão, portanto, aplicar-se ao conteúdo de ficheiros digitais, como ficheiros multimédia ou livros eletrónicos ou o mero código-fonte do *software*». Tal não exclui que os fabricantes possam ser responsabilizados ao abrigo do direito nacional em matéria de responsabilidade civil.

2.5. **Conexão de dados**

26. O artigo 2.º, n.º 1, estabelece que o Regulamento de Ciber-Resiliência «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». Por conseguinte, o âmbito de aplicação do Regulamento de Ciber-Resiliência não se baseia na mera presença de dispositivos eletrónicos, mas na capacidade de um produto com elementos digitais para proceder ao intercâmbio de informações digitais.

27. Embora os termos «conexão lógica» e «conexão física» estejam definidos no artigo 3.º, o Regulamento de Ciber-Resiliência não define «conexão de dados» nem «dados digitais». Por conseguinte, é útil apresentar uma interpretação do que constitui uma conexão de dados, a fim de clarificar os limites do âmbito de aplicação do Regulamento de Ciber-Resiliência. Esta fronteira é especialmente importante para distinguir os produtos com elementos digitais que apenas utilizam sinais elétricos dos que participam na comunicação digital e, por conseguinte, estão expostos a riscos de cibersegurança.

28. Ao seu nível mais básico, uma conexão de dados implica a transmissão de informações sob forma binária, ou seja, como uma sequência de zeros e uns. Apenas ligar e desligar uma saída (ou seja, 0/1) não constitui, por si só, uma conexão de dados se esses estados não se destinarem a representar dados ou não forem lidos por uma entrada de dados digital. Para que exista uma conexão de dados, uma fonte deve codificar deliberadamente os estados binários como informação e devem poder ser descodificados como informação no destino. Por outras palavras, deve existir um remetente que crie deliberadamente símbolos digitais de acordo com um esquema definido e um recetor capaz de interpretar esses símbolos como dados. Quando são utilizados sinais elétricos ou eletrónicos exclusivamente para ativar ou alimentar uma função, sem transmitir informações codificadas digitalmente, não existe qualquer conexão de dados para efeitos do Regulamento de Ciber-Resiliência e, por conseguinte, o produto com elementos digitais não é abrangido pelo âmbito de aplicação do artigo 2.º, n.º 1.

2.6. **Sistemas complexos**

29. Os produtos com elementos digitais abrangidos pelo âmbito de aplicação do Regulamento de Ciber-Resiliência podem consistir não só em dispositivos ou componentes de *software* únicos, mas também em sistemas complexos, incluindo sistemas compostos por vários elementos de *hardware* e *software* que funcionam em conjunto para desempenhar uma determinada função. Caso um sistema deste tipo seja colocado no mercado como um produto único com elementos digitais, constitui um produto com elementos digitais na aceção do Regulamento de Ciber-Resiliência.

30. Estes sistemas complexos são frequentemente caracterizados por longos ciclos de conceção e desenvolvimento, com contratos que podem ter sido assinados antes do início da aplicação do Regulamento de Ciber-Resiliência, períodos de vida operacional alargados e um elevado grau de complexidade técnica e organizativa. Esses sistemas, a colocar no mercado após o início da aplicação do Regulamento de Ciber-Resiliência, podem basear-se em componentes colocados no mercado antes do início da aplicação desse regulamento, em arquiteturas estabelecidas ou em normas de interoperabilidade amplamente utilizadas, incluindo normas referidas noutros atos legislativos da UE ou em quadros setoriais. Consequentemente, modificar determinadas características técnicas desses sistemas pode ser difícil ou desproporcionado sem afetar a sua finalidade prevista, segurança, fiabilidade ou interoperabilidade com a infraestrutura existente.

31. Estas características não excluem, por si só, os sistemas complexos do âmbito de aplicação do Regulamento de Ciber-Resiliência. Pelo contrário, ilustram a aplicação da abordagem baseada no risco do Regulamento de Ciber-Resiliência, que permite demonstrar a conformidade de diferentes formas em função das características e dos condicionalismos do produto com elementos digitais, em conformidade com o artigo 13.º, n.º 3, do Regulamento de Ciber-Resiliência. Estas características fazem parte da sua finalidade prevista e do seu contexto operacional e, por conseguinte, são pertinentes para avaliar a conformidade com os requisitos essenciais de cibersegurança («requisitos essenciais»). Em especial, o considerando 55 reconhece explicitamente que determinados requisitos essenciais podem não ser plenamente compatíveis com a natureza de um produto com elementos digitais. Por exemplo, pode ser o caso se a conformidade for suscetível de comprometer os requisitos de interoperabilidade obrigatórios ou o bom funcionamento do sistema.

32. Por conseguinte, os fabricantes são obrigados a dar resposta aos riscos de cibersegurança com base na avaliação dos mesmos, a que se refere o artigo 13.º, n.º 2. Conforme também explicado no considerando 55, em alguns casos, determinados requisitos essenciais específicos não são aplicáveis ou não podem ser cumpridos através da aplicação

de medidas de segurança de ponta devido, por exemplo, à finalidade prevista do sistema, que exige que o produto com elementos digitais interaja com dependências existentes ou cumpra determinados requisitos de interoperabilidade. Nesses casos, os fabricantes devem identificar e documentar esses condicionalismos específicos, avaliar os riscos associados e aplicar medidas alternativas ou compensatórias adequadas de atenuação dos riscos, de modo a não comprometer a segurança do produto com elementos digitais. Para o efeito, tanto a documentação técnica referida no artigo 31.º como as informações e instruções destinadas ao utilizador referidas no anexo II desempenham um papel fundamental na descrição transparente dos condicionalismos identificados, dos riscos de cibersegurança conexos e das medidas de atenuação dos riscos aplicadas. Em conformidade com a obrigação de manter atualizada a avaliação dos riscos durante o período de apoio, os fabricantes devem também reavaliar periodicamente se esses condicionalismos continuam a existir. Caso esses condicionalismos possam ser removidos ou reduzidos ao longo do tempo, os fabricantes devem atualizar o produto com elementos digitais em conformidade, para que possa avançar para um nível adequado de cibersegurança ([10]).

Exemplo 10: um fabricante coloca no mercado um produto com elementos digitais que comunica com sistemas externos utilizando um protocolo de rede. No âmbito da aplicação dos requisitos essenciais, o fabricante determina, com base na avaliação dos riscos de cibersegurança, que é necessária a utilização de um protocolo de comunicação seguro para garantir a confidencialidade e a integridade dos dados que são objeto de intercâmbio pelo produto com elementos digitais.

Todavia, a sua finalidade prevista inclui a interoperabilidade com sistemas existentes que apenas suportam um protocolo mais antigo ou menos seguro. Nesses casos, o fabricante pode aplicar esse protocolo caso tal seja necessário para viabilizar a interoperabilidade, desde que os riscos de cibersegurança conexos sejam identificados e atenuados por outros meios.

Caso seja tecnicamente viável que o produto com elementos digitais suporte tanto o protocolo seguro como o protocolo menos seguro, o fabricante deverá aplicar o protocolo seguro e permitir a sua utilização por defeito. O protocolo menos seguro só seria permitido quando necessário para a interoperabilidade.

Exemplo 11: um fabricante de um sistema de automatização industrial adquire alguns microcontroladores antes do início da aplicação do Regulamento de Ciber-Resiliência. O fabricante realiza a avaliação dos riscos de cibersegurança para que o seu sistema de automatização industrial seja colocado no mercado após o início da aplicação do regulamento. Com base nessa avaliação dos riscos de cibersegurança, o fabricante não identifica riscos de cibersegurança específicos associados à utilização de um desses microcontroladores. O fabricante integra-o no seu sistema de automatização industrial e assegura que o produto com elementos digitais no seu todo (o sistema de automatização industrial) cumpre os requisitos essenciais.

2.7. **Produtos com elementos digitais concebidos antes do início da aplicação do Regulamento de Ciber-Resiliência**

33. Em alguns casos, um fabricante colocará no mercado, após o início da aplicação do Regulamento de Ciber--Resiliência, em 11 de dezembro de 2027, unidades de um produto com elementos digitais fabricadas em conformidade com um tipo ou modelo concebido e desenvolvido antes da data de aplicação do Regulamento de Ciber-Resiliência. Nesses casos, a conformidade com o referido regulamento não exige necessariamente a reformulação dessas unidades do produto com elementos digitais. O fabricante é obrigado a realizar uma avaliação dos riscos de cibersegurança, por força do artigo 13.º, n.º 2, do Regulamento de Ciber-Resiliência, a fim de determinar, com base na finalidade prevista e na utilização razoavelmente previsível do produto com elementos digitais, quais dos requisitos essenciais constantes da parte I do anexo I são aplicáveis, e de que forma, a esse produto com elementos digitais.

34. Caso o resultado dessa avaliação dos riscos demonstre que o produto com elementos digitais já incorpora medidas de segurança adequadas e eficazes para dar resposta aos riscos pertinentes, o fabricante pode basear-se nessas medidas existentes para demonstrar a conformidade com o Regulamento de Ciber-Resiliência. Este regulamento não impõe, por si só, a obrigação de introduzir novos elementos de segurança ou de reformular o produto com elementos digitais sempre que tal não seja necessário para dar resposta aos riscos identificados.

([10]) Importa salientar que as considerações enunciadas no presente número podem ser aplicáveis, se for caso disso, a todos os produtos com elementos digitais abrangidos pelo âmbito de aplicação do Regulamento de Ciber-Resiliência e não apenas a «sistemas complexos».

35. Todavia, o fabricante continua sujeito às obrigações estabelecidas no Regulamento de Ciber-Resiliência. Estas incluem garantir, antes de o produto com elementos digitais ser colocado no mercado, que o procedimento de avaliação da conformidade aplicável foi realizado, que a declaração UE de conformidade foi elaborada e que a marcação CE foi aposta. O cumprimento desses requisitos é independente do facto de a conceção do produto com elementos digitais exigir modificações em resultado da avaliação dos riscos. No caso de produtos com elementos digitais concebidos antes da data de aplicação do Regulamento de Ciber-Resiliência, mas colocados no mercado após essa data, quando não for possível ao fabricante demonstrar de que forma a avaliação dos riscos foi tida em conta durante a fase de conceção e desenvolvimento do produto com elementos digitais, deve entender-se que a obrigação prevista no artigo 13.º, n.º 2, exige que os fabricantes realizem uma avaliação dos riscos de cibersegurança e demonstrem, nessa base, que o produto com elementos digitais incorpora medidas de segurança adequadas com vista a minimizar os riscos de cibersegurança, prevenir incidentes e minimizar o seu impacto, nomeadamente em relação à saúde e segurança dos utilizadores.

36. Por conseguinte, os produtos com elementos digitais concebidos antes do início da aplicação do Regulamento de Ciber-Resiliência podem ser colocados no mercado ao abrigo do Regulamento de Ciber-Resiliência sem reformulação, desde que o fabricante possa demonstrar, através da avaliação dos riscos de cibersegurança e da documentação técnica, que o produto com elementos digitais atinge um nível adequado de cibersegurança à luz da sua finalidade prevista e da sua utilização razoavelmente previsível, bem como que cumpre os requisitos essenciais de cibersegurança.

37. Além disso, é útil clarificar a aplicação das obrigações de avaliação da conformidade aos fabricantes de produtos com elementos digitais colocados no mercado após o início da aplicação do Regulamento de Ciber-Resiliência, mas fabricados em conformidade com um tipo ou modelo concebido e desenvolvido antes dessa data. Em conformidade com o artigo 13.º, n.º 12, o fabricante deve demonstrar, através do procedimento de avaliação da conformidade pertinente, que o seu produto com elementos digitais está em conformidade com os requisitos essenciais aplicáveis e incluir provas nesse sentido na documentação técnica do produto (ponto 6 do anexo VII).

38. No entanto, a aplicação desses requisitos deve ser interpretada à luz da avaliação dos riscos de cibersegurança e do perfil de risco de cibersegurança do produto com elementos digitais. Em especial no caso de produtos com elementos digitais concebidos antes da data de aplicação do Regulamento de Ciber-Resiliência (mas colocados no mercado após essa data) e sujeitos aos procedimentos de avaliação da conformidade previstos no artigo 32.º, n.º 1, se a avaliação dos riscos demonstrar que o produto com elementos digitais já incorpora medidas de segurança adequadas e eficazes para dar resposta aos riscos desse produto, não se deve entender que a obrigação de apresentar provas no âmbito do procedimento de avaliação da conformidade exige que o fabricante faculte resultados de ensaios que abranjam as fases iniciais de conceção e desenvolvimento desses produtos com elementos digitais. Tal não seria necessário, pois não contribuiria para aumentar a segurança do próprio produto com elementos digitais. Caso os ensaios sejam, mesmo assim, necessários, não se espera que os fabricantes apresentem provas dos ensaios realizados em todas as variantes do produto, mas podem agrupar esses ensaios em famílias de produtos com elementos digitais, conforme abordado mais pormenorizadamente na secção *7.4 Reutilização de avaliações dos riscos e de documentação de conformidade para famílias de produtos* com elementos digitais.

39. No entanto, o fabricante deve apresentar provas da forma como cumpre os processos de tratamento de vulnerabilidades estabelecidos na parte II do anexo I, deve manter a sua avaliação dos riscos atualizada em conformidade com o artigo 13.º, n.º 3, e deve cumprir todas as outras obrigações estabelecidas no Regulamento de Ciber-Resiliência, nomeadamente ao facultar aos utilizadores informações e instruções em conformidade com o artigo 13.º, n.º 18.

Exemplo 12: um fabricante coloca no mercado um microcontrolador que foi concebido e desenvolvido antes da data de aplicação do Regulamento de Ciber-Resiliência. O microcontrolador destina-se a ser integrado numa série de produtos eletrónicos com elementos digitais, incluindo produtos com elementos digitais com funcionalidades de conectividade.

Antes de colocar novas unidades do microcontrolador no mercado após o início da aplicação do Regulamento de Ciber-Resiliência, o fabricante realiza uma avaliação dos riscos de cibersegurança em conformidade com o artigo 13.º, n.º 2. Com base na finalidade prevista do microcontrolador e na sua utilização razoavelmente previsível, o fabricante identifica os riscos de cibersegurança pertinentes, como o acesso não autorizado, a manipulação de software *ou dados e a utilização abusiva das interfaces disponíveis.*

O resultado da avaliação dos riscos mostra que o microcontrolador, tal como foi originalmente concebido, já incorpora medidas de segurança adequadas e eficazes para dar resposta aos riscos identificados. Por conseguinte, o fabricante conclui que o produto com elementos digitais cumpre os requisitos essenciais pertinentes estabelecidos na parte I do anexo I e que não é necessária qualquer reformulação ou introdução de funcionalidades de segurança adicionais.

Caso não seja possível demonstrar de que forma uma avaliação dos riscos de cibersegurança foi tida em conta durante a fase inicial de conceção e desenvolvimento, o fabricante documenta uma avaliação dos riscos de cibersegurança em curso e explica de que forma a conceção e as medidas existentes atenuam os riscos identificados. O fabricante não é obrigado a recriar documentos históricos de conceção ou ensaio, pois tal não contribuiria para reforçar a cibersegurança do produto com elementos digitais. Caso diversas variantes do microcontrolador se baseiem na mesma conceção e partilhem o mesmo perfil de risco de cibersegurança, o fabricante pode também basear-se em provas representativas que abranjam a família de produtos em causa.

O fabricante assegura igualmente o cumprimento dos requisitos de tratamento de vulnerabilidades estabelecidos na parte II do anexo I, nomeadamente ao manter processos para resolver e corrigir vulnerabilidades, bem como ao manter a avaliação dos riscos de cibersegurança sob análise, em conformidade com o artigo 13.º, n.º 3.

Nestas circunstâncias, o microcontrolador concebido antes da data de aplicação do Regulamento de Ciber-Resiliência pode ser colocado no mercado sem reformulação, desde que o fabricante possa demonstrar, através da avaliação dos riscos de cibersegurança e da documentação técnica, que atinge um nível adequado de cibersegurança à luz da sua finalidade prevista e da sua utilização razoavelmente previsível, bem como cumpre os requisitos essenciais aplicáveis.

3. *SOFTWARE* LIVRE E DE CÓDIGO-FONTE ABERTO

40. Conforme recordado na secção *2.1 Colocação no mercado*, o Regulamento de Ciber-Resiliência é aplicável a produtos com elementos digitais que são disponibilizados no mercado da UE no âmbito de uma atividade comercial pela primeira vez (ou seja, «colocados no mercado»), bem como a qualquer caso subsequente que constitua a disponibilização desse mesmo produto com elementos digitais no mercado. O Guia Azul (secção 2.2) esclarece que deve entender-se «atividade comercial» como o fornecimento de bens, a título oneroso ou gratuito, no contexto de uma atividade económica e só pode ser apreciada caso a caso, tendo em conta a regularidade dos fornecimentos, as características do produto, as intenções do fornecedor, etc.

41. O fornecimento no âmbito de uma atividade comercial caracteriza-se por uma série de circunstâncias, amplamente documentadas no Guia Azul e recordadas no considerando 15 do Regulamento de Ciber-Resiliência. Podem incluir a cobrança direta de um preço, bem como a «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» (considerando 15) ([11]).

42. Todavia, o Regulamento de Ciber-Resiliência reconhece as especificidades das diferentes formas de desenvolvimento e publicação de «*software* livre e de código-fonte aberto» (SL/A) e proporciona algumas orientações para ajudar a identificar se um SL/A é um produto com elementos digitais colocado no mercado (ou seja, no âmbito de uma atividade comercial) na aceção do Regulamento de Ciber-Resiliência. Conforme explicado no considerando 18, «[a]s meras circunstâncias em que o produto com elementos digitais foi desenvolvido ou a forma como o desenvolvimento foi financiado não deverão [...] ser tidas em conta para determinar a natureza comercial ou não comercial da atividade em causa». Mais especificamente, «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».

([11]) Importa igualmente recordar que, embora seja frequente os produtos com elementos digitais serem monetizados (também) através do tratamento de dados pessoais, a proteção dos dados pessoais é um direito fundamental e, por conseguinte, não podem ser considerados um produto de base, conforme indicado no considerando 24 da Diretiva (UE) 2019/770 do Parlamento Europeu e do Conselho, de 20 de maio de 2019, sobre certos aspetos relativos aos contratos de fornecimento de conteúdos e serviços digitais (JO L 136 de 22.5.2019, p. 1, ELI: http://data.europa.eu/eli/dir/2019/770/oj).

43. Por conseguinte, é útil i) clarificar o que é o SL/A, ii) explicar quando se considera que é da responsabilidade de uma pessoa singular ou coletiva e iii) facultar exemplos para ajudar as partes interessadas a compreender quando a distribuição de SL/A constitui uma colocação no mercado. Caso não seja colocado no mercado, o SL/A não é abrangido pelo âmbito de aplicação do Regulamento de Ciber-Resiliência, a menos que a entidade que o publica seja uma pessoa coletiva que corresponda à definição de «administrador de *software* de código-fonte aberto» (a seguir designado por «administrador») nos termos do artigo 3.º, ponto 14. Nesse caso, aplicam-se apenas as obrigações previstas no artigo 24.º.

44. No artigo 3.º, ponto 48, define-se o SL/A como «*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». Embora as presentes orientações não identifiquem licenças gratuitas e de código-fonte aberto específicas que sejam compatíveis com a definição estabelecida no artigo 3.º, ponto 48, decorre da redação dessa disposição que apenas o *software* que preencha cumulativamente duas condições pode ser considerado SL/A para efeitos do Regulamento de Ciber-Resiliência: i) o *software* deve ser disponibilizado ao abrigo de uma licença gratuita e de código-fonte aberto que conceda o conjunto completo de direitos a que se refere o artigo 3.º, ponto 48, e ii) o seu código-fonte deve ser partilhado abertamente.

45. O requisito de que a licença preveja que o *software* seja «livremente acessível, utilizável, modificável e redistribuível» reflete o entendimento tradicional de «SL/A», a saber, que os utilizadores devem poder aceder ao código-fonte, utilizá-lo sem restrições indevidas, modificá-lo e redistribuir versões originais ou modificadas. Por conseguinte, o acesso ao código-fonte é uma condição prévia necessária para o exercício dos outros direitos: sem acesso ao código-fonte, não é possível, de uma forma prática, modificar ou reutilizar significativamente o *software*.

46. No entanto, o artigo 3.º, ponto 48, vai além da mera referência às condições da licença, pois exige expressamente que o código-fonte seja «partilhado abertamente». O conceito de «partilhado abertamente» indica que o código-fonte deve ser disponibilizado ao público («a montante» ou «a jusante») e não apenas fornecido de forma restrita ou condicional. Por conseguinte, o *software* distribuído ao abrigo de uma licença gratuita e de código-fonte aberto, mas cujo código-fonte só é partilhado (ou autorizado a ser partilhado) com clientes pagadores ou com um grupo limitado de utilizadores, não deve ser considerado um SL/A na aceção do artigo 3.º, ponto 48. Por conseguinte, para efeitos do Regulamento de Ciber-Resiliência, só deve ser considerado como SL/A o *software* cujo código-fonte esteja disponível ao público e licenciado ao abrigo de uma licença gratuita e de código-fonte aberto que conceda o conjunto completo de direitos a que se refere o artigo 3.º, ponto 48.

3.1. **Determinar se o *software* livre e de código-fonte aberto está sob a sua responsabilidade**

47. O Regulamento de Ciber-Resiliência atribui responsabilidades fundamentais aos operadores económicos que fornecem produtos com elementos digitais no mercado da UE. Define o fabricante como a pessoa singular ou coletiva que fornece um produto com elementos digitais em seu nome ou sob a sua marca e que o faz no âmbito de uma atividade comercial (colocando-o assim no mercado). Do mesmo modo, um importador é a pessoa singular ou coletiva estabelecida na UE que fornece o produto com elementos digitais de uma pessoa estabelecida fora da UE e que o faz no âmbito de uma atividade comercial (colocando-o assim no mercado). As obrigações dos administradores aplicam-se à pessoa coletiva que fornece um SL/A destinado a atividades comerciais ([12]), mas que não o coloca no mercado na aceção do Regulamento de Ciber-Resiliência.

48. Por conseguinte, para determinar se uma pessoa singular ou coletiva está a colocar o SL/A no mercado da UE, é necessário clarificar, em primeiro lugar, se essa pessoa singular ou coletiva efetivamente fornece o SL/A. A fim de estabelecer corretamente as obrigações aplicáveis por força do Regulamento de Ciber-Resiliência, é essencial determinar se a pessoa singular ou coletiva efetivamente realiza a operação de fornecimento de um SL/A. Com efeito, conforme recordado no considerando 18, o Regulamento de Ciber-Resiliência não se aplica às pessoas singulares ou coletivas que contribuam com código-fonte para produtos com elementos digitais considerados SL/A que não estejam sob a sua responsabilidade.

([12]) Trata-se de uma condição necessária, mas não suficiente, para que uma pessoa coletiva possa ser considerada um administrador de *software* de código-fonte aberto, uma vez que a definição constante do artigo 3.º, ponto 14, estabelece condições adicionais para que uma pessoa coletiva possa ser considerada um administrador.

49. Tendo em conta as especificidades do desenvolvimento do SL/A, que envolve frequentemente vários contribuintes, modelos de colaboração descentralizados e uma separação entre a contribuição e a tomada de decisões, é útil clarificar que o SL/A é considerado «sob a responsabilidade» das pessoas singulares ou coletivas que o publicam e exercem o controlo principal sobre as suas decisões de desenvolvimento, lançamento e distribuição (frequentemente designadas por «responsáveis pela manutenção»). As pessoas que contribuem com código-fonte, mas que não controlam lançamentos, roteiros ou decisões de governação, são consideradas «contribuintes». Nesses casos, o SL/A não está sob a sua responsabilidade, embora tenham contribuído com código para o mesmo. A mera existência de autorizações técnicas, como a autorização de acesso, não é suficiente para estabelecer que o SL/A está sob a responsabilidade dessa pessoa, pois a responsabilidade cabe a quem publica e controla o SL/A.

Exemplo 13: um criador individual ou um trabalhador de uma empresa apresenta um pedido de «extração» ou «fusão» que contém uma atualização corretiva de segurança ou uma nova funcionalidade para o projeto de um SL/A. Os responsáveis pela manutenção do projeto analisam, aceitam e fundem o código no repositório principal, incluindo-o posteriormente numa nova versão. Neste cenário, a pessoa que apresentou o pedido de extração é um «contribuinte» e não está sujeito ao Regulamento de Ciber-Resiliência. Embora essa pessoa tenha contribuído com código-fonte, não exerce o controlo principal sobre as decisões de desenvolvimento, lançamento ou distribuição.

3.2. **Determinar se o *software* livre e de código-fonte aberto é colocado no mercado da UE**

50. Após se estabelecer que um SL/A está sob a responsabilidade de uma pessoa singular ou coletiva, é necessário determinar se essa pessoa o fornece no âmbito de uma atividade comercial, constituindo assim uma colocação no mercado.

3.2.1. *Cobrança de um preço*

51. Caso a pessoa singular ou coletiva que fornece um SL/A cobre um preço pelo próprio *software* (por exemplo, cobrando um preço pelos binários pré-compilados), essa pessoa está a colocar um produto com elementos digitais no mercado. Por conseguinte, ao abrigo do Regulamento de Ciber-Resiliência, a pessoa que coloca um SL/A no mercado é um fabricante.

52. Muitas vezes, os fabricantes de SL/A fornecem versões gratuitas desse *software* (frequentemente designadas versões «comunitárias»), cuja base de códigos é (quase) idêntica à versão paga. Todavia, esses produtos com elementos digitais são produtos diferentes: a versão paga é monetizada de alguma forma (por exemplo, cobrando um preço ou através de outros meios, como referido na presente secção) e, por conseguinte, considerada colocada no mercado, desencadeando as obrigações do fabricante. A versão fornecida gratuitamente (ou versão comunitária) não é monetizada e, por conseguinte, para efeitos do Regulamento de Ciber-Resiliência, não é considerada colocada no mercado. É também o que acontece quando a versão paga é uma versão comercial «melhorada», que alarga a base de códigos da versão fornecida gratuitamente, ou incorpora essa versão num produto mais vasto com elementos digitais (por exemplo, como no caso do modelo «*open core*»).

53. Se a pessoa que fornece a versão comunitária for uma pessoa coletiva, essa pessoa coletiva está igualmente sujeita às obrigações dos administradores relativamente à versão que fornece gratuitamente (versão comunitária). Se a entidade for uma pessoa singular, a versão fornecida gratuitamente (a versão comunitária) não é abrangida pelo âmbito de aplicação do Regulamento de Ciber-Resiliência.

3.2.2. *Monetização de outros serviços ou exigência do tratamento de dados pessoais*

54. Uma pessoa singular ou coletiva que publique um SL/A também pode colocá-lo no mercado (ou seja, fornecê-lo no âmbito de uma atividade comercial) caso forneça o *software* através do qual monetiza outros produtos com elementos digitais ou serviços, ou se exigir, como condição para a utilização, o tratamento de dados pessoais por razões que não sejam exclusivamente destinadas a melhorar a segurança, a compatibilidade ou a interoperabilidade do *software*.

Exemplo 14: uma pessoa singular ou coletiva publica uma aplicação de mercado em linha livre e de código-fonte aberto. A aplicação está disponível gratuitamente e permite aos utilizadores adquirir bens ou serviços através da mesma. A aplicação permite à pessoa que a publicou monetizar outros produtos com elementos digitais e serviços oferecidos por meio da mesma (por exemplo, através de anúncios, comissões ou taxas de subscrição). Por conseguinte, considera-se que a aplicação foi colocada no mercado no âmbito de uma atividade comercial.

Exemplo 15: uma pessoa singular ou coletiva publica uma rede privada virtual (VPN) livre e de código-fonte aberto. A aplicação está disponível gratuitamente, mas permite que os utilizadores paguem para aceder a endereços IP específicos ou servidores adicionais. Essa aplicação permite a essa pessoa monetizar outros serviços oferecidos através da mesma, pelo que se considera que foi colocada no mercado no âmbito de uma atividade comercial.

Exemplo 16: uma pessoa singular ou coletiva publica uma aplicação de monitorização de atividade física livre e de código-fonte aberto. A aplicação é disponibilizada gratuitamente, mas a sua utilização está subordinada ao tratamento dos dados pessoais dos utilizadores para fins como publicidade direcionada ou análises não relacionados com a segurança, a compatibilidade ou a interoperabilidade do software*. Ao exigir esse tratamento de dados como condição de utilização, considera-se, por conseguinte, que a aplicação foi colocada no mercado no âmbito de uma atividade comercial.*

3.2.3. *Serviços de apoio*

55. O simples facto de uma pessoa singular ou coletiva que publica um SL/A também oferecer serviços de apoio pagos relacionados com o mesmo não significa, por si só, que o produto com elementos digitais seja fornecido no âmbito de uma atividade comercial. Os serviços de apoio podem incluir atividades como consultoria, formação ou serviços profissionais relacionados com a utilização, documentação, configuração e implantação do *software* por um cliente.

56. O fator decisivo consiste em saber se o acesso ao próprio SL/A (ou seja, a produção do produto com elementos digitais), incluindo a sua manutenção, está condicionado a uma remuneração, e não à mera oferta de serviços profissionais em torno de um produto com elementos digitais livremente disponível, como indicado no considerando 18 do Regulamento de Ciber-Resiliência («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»). Caso o SL/A possa ser descarregado e instalado gratuitamente e os utilizadores possam optar por adquirir serviços profissionais separadamente, considera-se que esse SL/A não é colocado no mercado.

57. Em contrapartida, em alguns casos, o acesso a uma versão específica do produto com elementos digitais, incluindo determinados benefícios, como a assistência técnica ou a otimização do desempenho, está condicionado à remuneração. Nesses casos, esse fornecimento constitui um fornecimento monetizado de um produto com elementos digitais no âmbito de uma atividade comercial e, por conseguinte, considera-se que foi colocado no mercado. Incluem-se casos em que uma edição paga ou uma versão empresarial é disponibilizada ao abrigo de um acordo comercial, independentemente de também estar disponível, a título gratuito, *software* funcionalmente equivalente ao abrigo de uma licença gratuita e de código-fonte aberto.

Exemplo 17: uma pessoa singular ou coletiva publica um sistema operativo livre e de código-fonte aberto, oferecendo uma versão paga desse sistema operativo que inclui serviços de apoio, como assistência técnica ou otimização do desempenho. Considera-se que a versão paga do sistema operativo foi colocada no mercado no âmbito de uma atividade comercial.

Exemplo 18: uma pessoa singular ou coletiva publica uma ferramenta de linha de comandos livre e de código-fonte aberto. A ferramenta é de acesso livre e qualquer pessoa pode descarregá-la e instalá-la. Essa pessoa singular ou coletiva presta, separadamente, serviços profissionais, como serviços de consultoria opcionais para ministrar formação aos utilizadores e apoiá-los na instalação e utilização da ferramenta. Esse SL/A não é considerado colocado no mercado na aceção do Regulamento de Ciber-Resiliência.

58. Em especial no caso de pessoas singulares que publicam SL/A, a prestação de assistência técnica diretamente associada ao acesso ao produto com elementos digitais continuará a não ser considerada uma atividade comercial se, conforme indicado no considerando 15 do Regulamento de Ciber-Resiliência, o preço cobrado servir apenas para a recuperação dos custos reais. Esses custos reais incluem uma variedade de custos relacionados com a conceção, o desenvolvimento e a manutenção desse *software*, incluindo as despesas razoáveis de subsistência da pessoa. Por conseguinte, uma pessoa singular que publique um SL/A e preste assistência técnica para cobrir os seus custos, bem como para obter uma remuneração justa, não deve ser considerada, apenas por esse motivo, como uma colocação desse *software* no mercado da UE.

59. Não se considera que uma pessoa singular ou coletiva que preste assistência técnica relacionada com um SL/A que não esteja sob a sua responsabilidade coloque esse *software* no mercado, a menos que essa pessoa modifique substancialmente o SL/A, em conformidade com o artigo 22.º, no âmbito da sua prestação dessa assistência.

Exemplo 19: um prestador de serviços não publica um SL/A, mas ajuda um cliente a instalá-lo no servidor local deste último. Fá-lo sem proceder a uma modificação substancial desse SL/A. Por conseguinte, não se considera que o prestador de serviços coloque o SL/A no mercado.

3.2.4. *Donativos*

60. É habitual as pessoas singulares ou coletivas que publicam projetos de SL/A incluírem formas de os utilizadores desse *software* doarem dinheiro, a título voluntário, para agradecer ao(s) editor(es) do projeto e também para assegurar que o projeto continua a ser ativamente mantido.

61. Conforme indicado no considerando 15 do Regulamento de Ciber-Resiliência, «[a] aceitação de donativos sem intenção de fazer lucro não deverá ser considerada uma atividade comercial». O simples facto de incluir uma ligação para uma plataforma de donativos, ou ferramentas semelhantes para recolher donativos, não deve ser visto como uma intenção de obter lucro, mesmo que o montante recolhido através de donativos exceda os meros custos associados à conceção, ao desenvolvimento e ao fornecimento de um produto com elementos digitais. Tal inclui uma compensação razoável para os contribuintes contratados por uma pessoa coletiva e/ou para as despesas razoáveis de subsistência de uma pessoa singular. Os donativos, pela sua própria natureza, variam ao longo do tempo, pelo que deve ser exercido um certo grau de flexibilidade ao avaliar se se considera que um SL/A monetizado exclusivamente através de donativos foi colocado no mercado. Por conseguinte, é pouco provável que um SL/A apoiado apenas através de donativos seja considerado colocado no mercado na aceção do Regulamento de Ciber-Resiliência.

Exemplo 20: uma pessoa singular ou coletiva publica uma ferramenta de SL/A num repositório público em linha, permitindo a qualquer pessoa descarregá-la, utilizá-la, modificá-la e redistribuí-la ao abrigo de uma licença gratuita e de código-fonte aberto. O editor convida os utilizadores a fazerem donativos voluntários através de uma plataforma de donativos, a fim de apoiar o desenvolvimento e a manutenção contínuos do projeto. O acesso ao software*, ao respetivo código-fonte e às suas atualizações não está subordinado à realização de um donativo. O SL/A não é considerado fornecido no âmbito de uma atividade comercial e não é considerado colocado no mercado na aceção do Regulamento de Ciber-Resiliência.*

62. Todavia, há casos em que se pode considerar que um SL/A apoiado através de donativos foi colocado no mercado. É o que acontece quando, com base numa avaliação global das circunstâncias, os donativos são de facto equivalentes à cobrança de um preço para aceder ao produto com elementos digitais ou a algumas das respetivas funcionalidades. Tal pode ser o caso, em especial, quando o acesso ao SL/A, a funcionalidades essenciais ou a atualizações é condicionado, na prática, à realização de um donativo, ou quando os donativos estão associados a benefícios contratuais ou vantagens exclusivas que vão além dos interesses da comunidade.

Exemplo 21: uma pessoa singular ou coletiva publica um produto de software *com elementos digitais ao abrigo de uma licença gratuita e de código-fonte aberto, mas fornece versões descarregáveis e atualizações de segurança apenas aos utilizadores que fazem um donativo. Os utilizadores que não fizerem um donativo não têm acesso à versão atual do* software.

Neste caso, os donativos são, de facto, uma condição para o acesso ao produto com elementos digitais e, por conseguinte, equivalem à cobrança de um preço. Por conseguinte, considera-se que o SL/A foi colocado no mercado na aceção do Regulamento de Ciber-Resiliência.

Exemplo 22: uma pessoa singular ou coletiva disponibiliza publicamente o código-fonte de um SL/A, mas fornece binários pré-compilados, atualizações periódicas e correções de segurança garantidas apenas aos doadores. Neste caso, os donativos estão associados ao acesso a aspetos essenciais do produto com elementos digitais e constituem uma remuneração pelo fornecimento desse produto. Por conseguinte, considera-se que esse SL/A foi colocado no mercado no âmbito de uma atividade comercial.

3.2.5. *Financiamento do* software *livre e de código-fonte aberto*

63. O simples facto de um terceiro ter pagado, patrocinado ou financiado de outra forma o desenvolvimento de um SL/A não determina, por si só, se esse SL/A é colocado no mercado. É prática comum no ecossistema dos SL/A que os criadores individuais, fundações ou comunidades recebam financiamento de empresas, organismos públicos ou outros patrocinadores, a fim de trabalhar em características específicas, corrigir erros ou manter componentes críticos. Este financiamento pode assumir muitas formas, incluindo subvenções, recompensas por deteção de erros de programação, patrocínios, contratos de prestação de serviços ou trabalhos de desenvolvimento remunerados.

64. Conforme já recordado, o considerando 18 do Regulamento de Ciber-Resiliência clarifica que as meras circunstâncias em que o produto com elementos digitais foi desenvolvido ou a forma como o desenvolvimento foi financiado não deverão ser tidas em conta para determinar a natureza comercial da atividade em causa.

65. Por conseguinte, caso o SL/A seja partilhado abertamente e disponibilizado gratuitamente a todos para que acedam, utilizem, modifiquem e redistribuam, o facto de uma entidade comercial poder ter pagado por esse projeto não deverá contribuir para determinar se o *software* é colocado no mercado. Com efeito, se esse SL/A não for monetizado de outra forma, não deve ser considerado como colocado no mercado. Caso a empresa que financiou o desenvolvimento do SL/A (bem como qualquer outra empresa) o integre no seu produto com elementos digitais, essa empresa deve exercer a diligência devida em conformidade com o artigo 13.º, n.º 5, do Regulamento de Ciber-Resiliência.

Exemplo 23: um criador individual publica um projeto de SL/A e mantém-no ativamente. O fabricante A solicita que o criador individual adicione uma funcionalidade específica a esse SL/A e financia esse desenvolvimento. O criador adiciona a funcionalidade à base de códigos do SL/A, partilhando-a abertamente e disponibilizando-a livremente a todos para acederem, utilizarem, modificarem e redistribuírem. Não se considera que o criador individual tenha colocado esse SL/A no mercado. Se o fabricante integrar o SL/A no seu produto com elementos digitais, deve exercer a diligência devida em conformidade com o artigo 13.º, n.º 5.

3.2.6. *Entidades sem fins lucrativos criadas para alcançar objetivos sem fins lucrativos*

66. Se uma pessoa coletiva que publica um SL/A for uma organização sem fins lucrativos «criada de forma a garantir que todas as receitas após os custos sejam utilizadas para alcançar objetivos sem fins lucrativos» (considerando 18 do Regulamento de Ciber-Resiliência), o SL/A que publica não é considerado colocado no mercado. Se essa pessoa coletiva corresponder à definição de «administrador», está sujeita às obrigações correspondentes (artigo 24.º do Regulamento de Ciber-Resiliência).

Exemplo 24: uma pessoa coletiva publica um navegador livre e de código-fonte aberto que é diretamente monetizado através de parcerias com motores de pesquisa, mas todas as suas receitas após os custos são utilizadas para objetivos sem fins lucrativos. O navegador não é considerado colocado no mercado na aceção do Regulamento de Ciber-Resiliência. A pessoa coletiva que o publica está sujeita às obrigações aplicáveis aos administradores.

3.2.7. *Integração por outros fabricantes*

67. Em alguns casos, um SL/A é publicado por uma pessoa singular ou coletiva claramente identificável, mas esse SL/A destina-se «à integração por outros fabricantes nos seus próprios produtos com elementos digitais». Nesses casos, considera-se que o SL/A não é colocado no mercado da UE, a menos que também seja monetizado pela pessoa que o publica (ou seja, o fabricante original), em conformidade com as secções anteriores das presentes orientações.

68. Caso esse SL/A não seja colocado no mercado, a pessoa coletiva que o publica estará sujeita às obrigações dos administradores, se prestar apoio contínuo, em consonância com a definição de «administrador».

Exemplo 25: uma pessoa coletiva publica uma biblioteca de SL/A para a construção de interfaces de utilizador. Não monetiza o fornecimento dessa biblioteca, mas integra-a num dos seus produtos com elementos digitais (que, por sua vez, é colocado no mercado). A biblioteca não é considerada colocada no mercado na aceção do Regulamento de Ciber-Resiliência, destinando-se a ser integrada em produtos com elementos digitais. A pessoa coletiva que a publica é o seu administrador.

Exemplo 26: uma pessoa coletiva coloca um sistema operativo no mercado e publica igualmente bibliotecas de SL/A que servem de implementações de referência para os utilizadores desse sistema operativo. A pessoa coletiva não monetiza as bibliotecas de SL/A, que se destinam a ser integradas noutros produtos com elementos digitais. A pessoa coletiva que as publica é um administrador dessas bibliotecas de SL/A.

3.3. **Administradores de *software* de código-fonte aberto**

69. O Regulamento de Ciber-Resiliência introduz a nova categoria jurídica de «administrador de *software* de código-fonte aberto» à luz da «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 [Regulamento de Ciber-Resiliência]» (considerando 19 do Regulamento de Ciber-Resiliência).

70. Em alguns casos, um SL/A é publicado, mas não disponibilizado no mercado, na aceção do Regulamento de Ciber-Resiliência, por uma pessoa coletiva «cujo propósito ou objetivo consiste em prestar apoio sistemático e contínuo ao desenvolvimento de [SL/A] [...] [destinado] a atividades comerciais, e que garante a viabilidade desses produtos» (artigo 3.º, ponto 14, do Regulamento de Ciber-Resiliência). Nesses casos, essa pessoa coletiva está sujeita às obrigações aplicáveis aos administradores.

71. Define-se «administrador» como «uma pessoa coletiva, que não um fabricante», uma vez que um fabricante, por definição, é a pessoa singular ou coletiva que coloca no mercado produtos com elementos digitais («os comercializa») em seu próprio nome ou sob a sua marca. Uma pessoa coletiva só pode ser administrador de produtos com elementos digitais que sejam considerados SL/A publicados, mas não disponibilizados no mercado na aceção do Regulamento de Ciber-Resiliência. Por conseguinte, o conceito de «administrador» aplica-se a casos específicos de SL/A «que, em última análise, se destinam a atividades comerciais, como a integração em serviços comerciais ou em produtos monetizados com elementos digitais» (considerando 19 do Regulamento de Ciber-Resiliência ([13])), mas não são disponibilizados no mercado na aceção do Regulamento de Ciber-Resiliência, e para os quais a pessoa coletiva que publica esse SL/A assegura um apoio sistemático.

72. Ser administrador de um SL/A específico não significa que essa pessoa coletiva também seja necessariamente administrador de outro SL/A que publica. Do mesmo modo, ser fabricante de um SL/A específico não significa que a pessoa coletiva não possa ser administrador de outro SL/A. Tal inclui a disponibilização de versões «comunitárias» do mesmo SL/A, conforme descrito na secção *3.2.1 Cobrança de um* preço.

73. Por conseguinte, uma pessoa coletiva pode ser simultaneamente administrador de um SL/A específico (presta apoio sistemático e contínuo e garante a viabilidade do *software*) e fabricante de outro SL/A específico (coloca-o no mercado). Por outras palavras, pode ser exigido à mesma entidade jurídica que desempenhe diferentes funções em diferentes projetos de SL/A.

74. Para cada SL/A específico que publique, a pessoa coletiva terá de determinar se esse SL/A é considerado colocado no mercado na aceção do Regulamento de Ciber-Resiliência. Em caso afirmativo, tal faz da entidade jurídica o fabricante do *software*. Se o SL/A não for considerado colocado no mercado, a pessoa coletiva pode ser o seu administrador, se o *software* se destinar a atividades comerciais e se a pessoa coletiva prestar apoio contínuo em consonância com a definição de administrador ([14]).

3.3.1. *Apoio contínuo e garantia da viabilidade do SL/A*

75. O considerando 19 explica que a prestação de apoio contínuo ao desenvolvimento de um produto com elementos digitais pode incluir (entre outros): i) o alojamento e a gestão de plataformas de colaboração para o desenvolvimento de *software*, ii) o alojamento de código-fonte ou *software*, iii) a administração ou gestão de produtos com elementos digitais que sejam considerados SL/A e iv) a orientação do desenvolvimento desses produtos com elementos digitais.

76. Tal pode ser o caso, por exemplo, de uma entidade jurídica que desenvolva o SL/A com o objetivo de o integrar nos seus próprios produtos com elementos digitais e, em seguida, o publica sem o colocar no mercado. Esta questão é igualmente abordada na secção *3.2.7 Integração por outros fabricantes*. Neste caso, a entidade jurídica não é um fabricante do *software*, mas pode ser um administrador do mesmo. Além disso, conforme explicado nas secções anteriores, uma entidade jurídica que publique uma versão gratuita (ou comunitária) e uma versão monetizada do mesmo SL/A é considerada um administrador da versão gratuita (ou comunitária) e um fabricante da versão monetizada.

77. Do mesmo modo, uma entidade jurídica que monetiza um SL/A, mas é uma entidade sem fins lucrativos cujas receitas após os custos são utilizadas para alcançar objetivos sem fins lucrativos (e, por conseguinte, o seu SL/A não é colocado no mercado na aceção do Regulamento de Ciber-Resiliência, como abordado na secção *3.2.6 Entidades sem* fins lucrativos), é administrador do SL/A que publica.

78. Além disso, determinadas fundações oferecem plataformas de colaboração com várias formas de governação, que permitem aos fabricantes contribuir periodicamente para o desenvolvimento do SL/A, e/ou que os fabricantes financiam periodicamente. Essas fundações devem ser consideradas administradores em relação a um SL/A específico que se destine a atividades comerciais e ao qual a fundação preste apoio contínuo. Todavia, conforme explicado na secção *3.3 Administradores de software* de código-fonte aberto, essa fundação não pode estar sujeita a quaisquer obrigações previstas no Regulamento de Ciber-Resiliência para outros SL/A específicos que aloje, nos casos em que não preste apoio sistemático a um SL/A específico, não garanta a sua viabilidade e/ou em que o *software* específico não se destine a atividades comerciais.

([13]) Este conceito está igualmente contido na formulação «se destinem a atividades comerciais» incluída na definição de «administrador de *software* de código-fonte aberto» estabelecida no artigo 3.º, ponto 14, do Regulamento de Ciber-Resiliência.

([14]) A pessoa coletiva também pode não estar sujeita a quaisquer obrigações nos termos do Regulamento de Ciber-Resiliência, caso: i) um SL/A específico não seja colocado no mercado na aceção do Regulamento de Ciber-Resiliência e ii) a entidade jurídica não corresponda à definição de administrador em relação a esse SL/A específico.

79. O tipo de «apoio contínuo» que as fundações e organizações semelhantes prestam a projetos específicos de SL/A pode variar consideravelmente. Por exemplo, determinadas entidades jurídicas apenas prestam apoio não técnico, como a gestão de marca dos projetos, o estabelecimento de regras de governação, a organização de eventos comunitários ou a recolha de donativos. Outras entidades também disponibilizam a infraestrutura informática subjacente necessária para executar o projeto, como o alojamento de repositórios de código-fonte, o fornecimento de sistemas de controlo de versões ou a geração de chaves de assinatura. Outras vão mais longe no tipo de apoio que prestam, contribuindo ativamente com recursos de engenharia para o projeto, por exemplo, ao empregar criadores, coordenar o trabalho de desenvolvimento, rever ou fundir códigos, gerir versões ou tratar de relatórios de vulnerabilidade e atualizações corretivas de segurança. Embora todas as entidades jurídicas que se qualificam como administradores nos termos do Regulamento de Ciber-Resiliência sejam obrigadas a cumprir as obrigações previstas no artigo 24.º, n.ºs 1 e 2, a medida em que as obrigações previstas no artigo 14.º, n.ºs 1, 3 e 8, se aplicam a essas entidades jurídicas varia em função do tipo de apoio que prestam, em conformidade com o artigo 24.º, n.º 3.

80. Por exemplo, um administrador que apenas preste apoio não técnico não participa, por definição, no desenvolvimento do produto com elementos digitais, pelo que não é obrigado a comunicar vulnerabilidades ativamente exploradas. Esse administrador também não disponibiliza quaisquer redes e sistemas de informação para o desenvolvimento desses produtos com elementos digitais, pelo que não é obrigado a comunicar incidentes graves à ENISA e às CSIRT, nem aos utilizadores afetados. Todavia, se o administrador tomar conhecimento de uma vulnerabilidade ativamente explorada (por exemplo, através de um relatório de fontes externas, como investigadores no domínio da segurança), deve partilhar as informações com os responsáveis pela manutenção do produto com elementos digitais, em conformidade com a sua política de cibersegurança. Os responsáveis pela manutenção dos produtos com elementos digitais e/ou os administradores também devem ponderar a comunicação voluntária da vulnerabilidade, em conformidade com o artigo 15.º.

81. Por outro lado, se um administrador fornecer a infraestrutura informática subjacente a determinados produtos com elementos digitais, é obrigado a notificar a ENISA e as CSIRT, por força do artigo 14.º, n.º 3, de quaisquer incidentes graves relacionados com essa infraestrutura que tenham impacto na segurança dos produtos com elementos digitais. É igualmente obrigado, se for caso disso, a informar todos os utilizadores (por exemplo, através de um anúncio geral). Conforme indicado no número anterior, embora o administrador não seja obrigado a comunicar vulnerabilidades ativamente exploradas de que tome conhecimento, deve promover o tratamento correto das vulnerabilidades e ponderar a transmissão voluntária de informações em conformidade com o artigo 15.º.

82. Por último, caso um administrador também forneça recursos de engenharia a produtos específicos com elementos digitais, é obrigado a: i) notificar, em conformidade com o artigo 14.º, n.º 1, das vulnerabilidades ativamente exploradas de que tome conhecimento e ii) se for caso disso, informar todos os utilizadores. Na medida em que o administrador também tenha uma relação direta com os utilizadores afetados, é igualmente obrigado a informá-los diretamente, em conformidade com o artigo 14.º, n.º 8.

83. Caso uma entidade deixe de prestar apoio sistemático e contínuo a um SL/A específico, pode deixar de corresponder à definição de administrador e, por conseguinte, deixar de estar sujeita às obrigações correspondentes. Nesses casos, essa entidade é incentivada a comunicar claramente a alteração do seu estatuto em relação a esse SL/A específico.

84. Em determinadas situações, uma entidade que tenha sido administradora de um projeto específico pode decidir monetizar diretamente esse projeto, colocando assim o produto com elementos digitais no mercado e desencadeando as obrigações aplicáveis ao fabricante por força do Regulamento de Ciber-Resiliência. Nessas circunstâncias, essa entidade é considerada o fabricante do produto com elementos digitais a partir da data em que o coloca no mercado (mas não em relação a versões anteriores para as quais atuou como administrador).

3.4. **Contribuintes e utilizações a jusante**

85. Conforme já referido na secção *3.1 Determinar se o software livre e de* código-fonte aberto está sob a sua responsabilidade, o Regulamento de Ciber-Resiliência clarifica que 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» (considerando 18).

86. Os fabricantes de produtos com elementos digitais que integrem componentes do SL/A nos seus próprios produtos com elementos digitais também não se tornam responsáveis pela conformidade individual desses componentes com o Regulamento de Ciber-Resiliência, mesmo que contribuam com código-fonte para a sua manutenção.

87. Do mesmo modo, o simples facto de os fabricantes integrarem componentes do SL/A nos seus próprios produtos (monetizados) com elementos digitais não tem impacto no estatuto desse componente do SL/A no âmbito do Regulamento de Ciber-Resiliência. Os responsáveis pela manutenção de componentes do SL/A que não são colocados no mercado não têm obrigações em relação a outras entidades que possam integrar esses componentes nos respetivos produtos com elementos digitais. A questão de saber se o Regulamento de Ciber-Resiliência se aplica a um determinado componente do SL/A depende exclusivamente de a pessoa singular ou coletiva que o publicou o colocar ou não no mercado.

88. Todavia, os fabricantes de produtos com elementos digitais que integrem componentes do SL/A são obrigados a cumprir o Regulamento de Ciber-Resiliência para os seus próprios produtos com elementos digitais. Têm igualmente uma obrigação de diligência devida, por força do artigo 13.º, n.º 5, em relação aos componentes do SL/A que integram. Além disso, são obrigados a comunicar vulnerabilidades em componentes integrados e a partilhar correções de segurança, por força do artigo 13.º, n.º 6. Para mais orientações sobre este tema, ver a secção *9.2.1 Comunicação de informações a montante e* partilha de correções de segurança.

3.5. **Cenários ilustrativos**

89. Os exemplos a seguir enumerados são completamente hipotéticos e destinam-se apenas a ilustrar diferentes casos explicados nas secções anteriores.

Exemplo 27: o criador individual A desenvolveu um SL/A. O criador A publica esse SL/A em seu próprio nome ou sob a sua marca, mas não cobra um preço pela sua utilização. O software *é partilhado abertamente e está livremente disponível para todos acederem, utilizarem, modificarem e redistribuírem. O criador A também inclui uma ligação para uma plataforma de recolha de donativos voluntários.*

As empresas B, C e D integram esse SL/A nos seus próprios produtos com elementos digitais. Para apoiar a manutenção contínua, as empresas B, C e D fazem donativos voluntários ao criador A. Estes donativos permitem a esse criador manter ativamente o projeto.

Esse SL/A não é colocado no mercado na aceção do Regulamento de Ciber-Resiliência. Este regulamento não impõe obrigações ao criador A. As empresas B, C e D devem exercer a diligência devida em conformidade com o artigo 13.º, n.º 5, ao integrarem esse SL/A nos seus próprios produtos com elementos digitais.

Exemplo 28: a fundação sem fins lucrativos F publica um componente de SL/A para integração noutros produtos comerciais com elementos digitais. A fundação F compromete-se a prestar apoio contínuo a esse SL/A, a fim de garantir a sua viabilidade e adoção. As empresas A, B e C integram esse SL/A nos seus próprios produtos com elementos digitais. As empresas A e B contribuem voluntariamente com algum tempo dos seus criadores para o desenvolvimento e a manutenção de projetos de SL/A no âmbito da fundação F, incluindo para esse SL/A.

Uma vez que a fundação F é uma entidade sem fins lucrativos criada de modo que as suas receitas após os custos sejam utilizadas para alcançar objetivos sem fins lucrativos, considera-se que o SL/A não é colocado no mercado na aceção do Regulamento de Ciber-Resiliência. A fundação F é o administrador do SL/A e está sujeita às obrigações correspondentes estabelecidas no artigo 24.º. As empresas A, B e C devem exercer a diligência devida em conformidade com o artigo 13.º, n.º 5, ao integrarem o SL/A nos seus próprios produtos com elementos digitais.

Exemplo 29: a empresa A desenvolveu um componente de SL/A para integração nos seus próprios produtos com elementos digitais. Também publica esse SL/A separadamente em seu próprio nome ou sob a sua marca e mantém-no ativamente. Todavia, não cobra pela sua utilização nem o monetiza de outras formas. As empresas B, C e D integram esse SL/A nos seus próprios produtos com elementos digitais e contribuem voluntariamente com algum tempo dos seus criadores para a respetiva manutenção.

Esse SL/A não é considerado colocado no mercado na aceção do Regulamento de Ciber-Resiliência. A empresa A não é o seu fabricante, mas sim o seu administrador. As empresas B, C e D devem exercer a diligência devida em conformidade com o artigo 13.º, n.º 5, ao integrarem o SL/A nos seus próprios produtos com elementos digitais.

Exemplo 30: a empresa A publica um SL/A em seu próprio nome ou sob a sua marca e oferece-o como versão paga, o que inclui determinados benefícios, como assistência técnica ou otimização do desempenho. Os criadores das empresas B, C e D contribuem para a manutenção do SL/A, mas este permanece sob o controlo da empresa A.

A empresa A é considerada fabricante desse SL/A ([15]). *As empresas B, C e D não estão sujeitas a obrigações decorrentes do Regulamento de Ciber-Resiliência para esse SL/A específico. Se integrarem esse SL/A nos seus próprios produtos com elementos digitais, são obrigadas a exercer a diligência devida, por força do artigo 13.º, n.º 5.*

Exemplo 31: a empresa A publica um SL/A em seu próprio nome ou sob a sua marca e assegura a manutenção contínua para garantir a sua viabilidade a longo prazo, a fim de permitir a integração desse software *nos produtos com elementos digitais de outras empresas. A empresa A não cobra pela sua utilização, não trata dados pessoais que recolhe através do produto com elementos digitais nem vende serviços de apoio associados à publicação do SL/A.*

A empresa B contribui com o código e o tempo dos criadores para a manutenção do SL/A, mas não o distribui comercialmente. A empresa B presta serviços de apoio técnico independentemente da distribuição do SL/A. Considera-se que a empresa A é administrador desse SL/A, ao passo que a empresa B não tem obrigações decorrentes do Regulamento de Ciber-Resiliência em relação a esse SL/A.

Exemplo 32: um componente do SL/A é publicado por uma entidade sem fins lucrativos criada de forma a assegurar que todas as receitas após os custos são utilizadas para alcançar objetivos sem fins lucrativos. A entidade presta apoio contínuo para garantir a viabilidade a longo prazo do projeto. A manutenção é financiada através de financiamento público, como subsídios de investigação. Outros desenvolvimentos, incluindo novas funcionalidades, são financiados através de donativos e projetos específicos, realizados em parceria com fabricantes que integram esse SL/A nos seus produtos com elementos digitais. Essas funcionalidades são incorporadas na base de códigos do SL/A.

A entidade sem fins lucrativos que publica o SL/A é considerada administrador desse componente do SL/A. Um fabricante que tenha contribuído para o desenvolvimento de determinadas funcionalidades não se torna o fabricante desse componente do SL/A. Caso o fabricante integre esse componente do SL/A no seu próprio produto com elementos digitais, deve exercer a diligência devida em conformidade com o artigo 13.º, n.º 5.

Exemplo 33: Uma entidade sem fins lucrativos criada de forma a assegurar que todas as receitas após os custos são utilizadas para alcançar objetivos sem fins lucrativos publica um conjunto de desenvolvimento de software *(SDK) de SL/A e assegura a sua manutenção contínua. O SDK é partilhado abertamente e está livremente disponível para todos acederem, utilizarem, modificarem e redistribuírem. O financiamento é concedido através de quotizações pagas à entidade sem fins lucrativos e os criadores empregados pelas organizações que são membros contribuem com código e outros recursos para o desenvolvimento do SDK. Os fabricantes utilizam o SDK como componente para criar outros produtos com elementos digitais.*

A entidade sem fins lucrativos que publica esse SDK é o seu administrador. Os membros da fundação não são responsáveis pelo cumprimento do Regulamento de Ciber-Resiliência por parte do SDK. Caso os fabricantes utilizem o SDK para construir o seu próprio produto com elementos digitais, devem exercer a diligência devida em conformidade com o artigo 13.º, n.º 5.

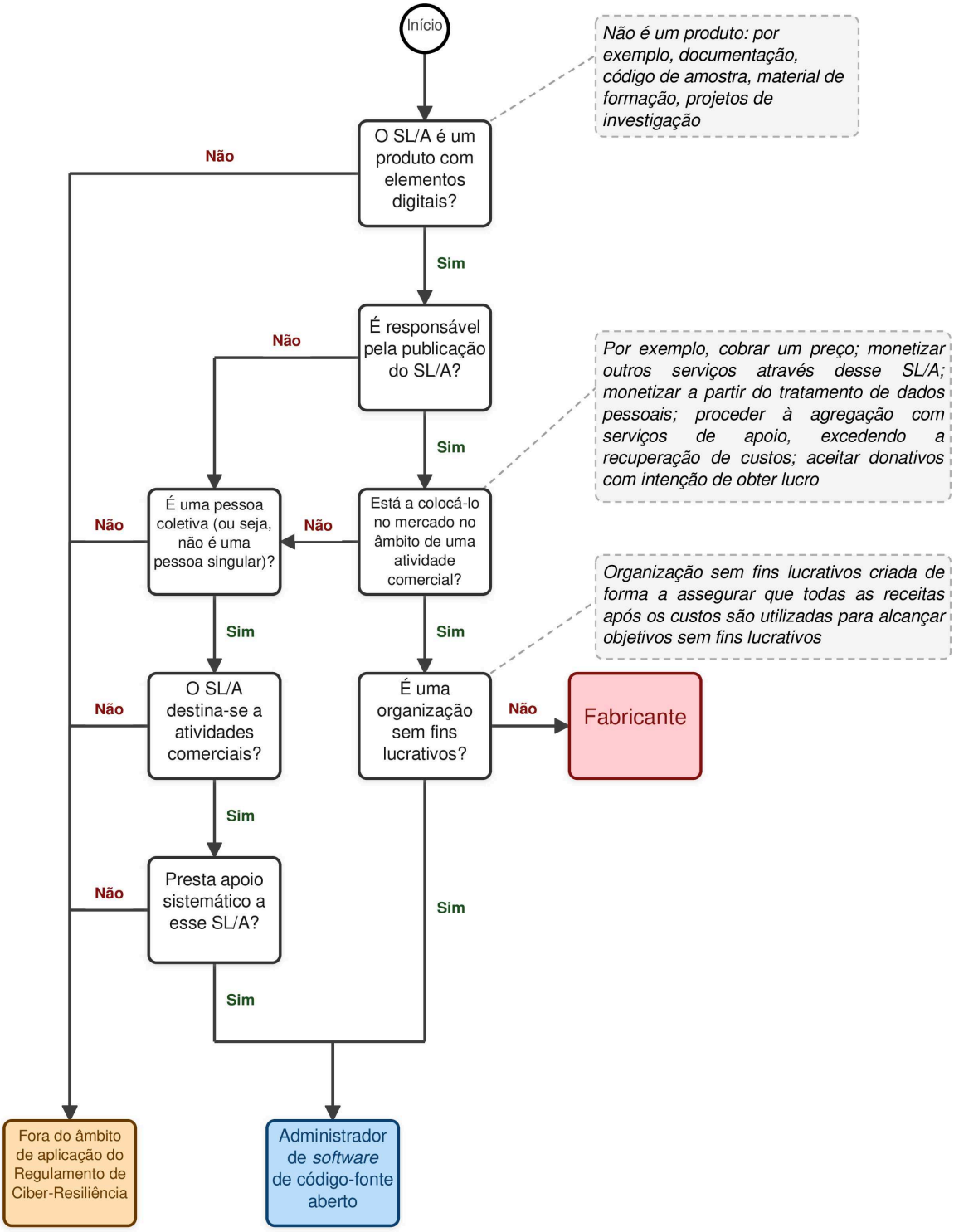
Exemplo 34: um criador individual publica uma biblioteca de SL/A num repositório público de pacotes para uma determinada linguagem de programação e mantém-na ativamente. Na documentação do pacote, o criador adiciona uma ligação para a recolha de donativos. Um fabricante descarrega gratuitamente essa biblioteca do repositório e integra-a no seu próprio produto com elementos digitais.

O Regulamento de Ciber-Resiliência não impõe obrigações ao criador individual nem ao repositório de pacotes. O fabricante que integra a biblioteca deve exercer a diligência devida em conformidade com o artigo 13.º, n.º 5.

([15]) A menos que a empresa A seja uma entidade sem fins lucrativos criada de forma a assegurar que todas as receitas após os custos são utilizadas para alcançar objetivos sem fins lucrativos, caso em que seria administrador desse SL/A.

Figura 1:

Fluxograma estilizado para a cobertura pelo Regulamento de Ciber-Resiliência de* software *livre e de código-fonte aberto



4. MODIFICAÇÕES SUBSTANCIAIS E PEÇAS SOBRESSELENTES

90. No artigo 3.º, ponto 30, do Regulamento de Ciber-Resiliência define-se «modificação substancial» como uma alteração do produto com elementos digitais após a sua colocação no mercado que i) afete a conformidade do produto com elementos digitais com os requisitos essenciais constantes da parte I do anexo I, ou ii) que resulte numa modificação da finalidade prevista para a qual o produto com elementos digitais foi avaliado.

91. A noção de modificação substancial é pertinente para determinar as obrigações constantes do Regulamento de Ciber-Resiliência numa série de casos, incluindo os seguintes:

a) Em conformidade com o artigo 21.º, um importador ou distribuidor que efetue uma modificação substancial de um produto com elementos digitais já colocado no mercado é considerado o seu fabricante;

b) Em conformidade com o artigo 22.º, qualquer pessoa singular ou coletiva que proceda a uma modificação substancial de um produto com elementos digitais e o disponibilize no mercado é considerada o seu fabricante;

c) Em conformidade com o artigo 69.º, n.º 2, qualquer pessoa singular ou coletiva que proceda a uma modificação substancial, após 11 de dezembro de 2027, de um produto com elementos digitais colocado no mercado antes de 11 de dezembro de 2027 e o coloque no mercado é considerada o seu fabricante;

d) Para fabricantes de produtos com elementos digitais colocados no mercado após 11 de dezembro de 2027, a fim de determinar se um produto com elementos digitais deve ser submetido a um novo procedimento de avaliação da conformidade devido a modificações efetuadas após essa data, em especial à luz da natureza iterativa do desenvolvimento de *software*.

92. Por conseguinte, é importante facultar orientações para ajudar os operadores económicos a compreender quando as modificações de *hardware* ou *software* podem ser consideradas modificações substanciais.

4.1. **Reparações físicas**

93. Conforme referido no considerando 42 do Regulamento de Ciber-Resiliência, «[s]e 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, 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 elementos 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». Tal é coerente com a secção 2.1 do Guia Azul, que recorda que «[u]m produto que tenha sido objeto de alterações ou transformações importantes após a sua entrada em serviço deve ser considerado um produto novo se: i) o seu desempenho inicial, a sua finalidade ou o seu tipo tiver sido alterado, sem que tal esteja previsto na avaliação inicial dos riscos, ii) a natureza do perigo tiver mudado ou o nível de risco tiver aumentado em relação à legislação de harmonização da União aplicável, e iii) o produto for disponibilizado (ou posto em serviço se a legislação aplicável abranger igualmente a entrada em serviço no seu âmbito de aplicação). É preciso avaliar caso a caso e, em especial, tendo em conta o objetivo da legislação e o tipo de produtos abrangidos pela legislação em causa».

94. As operações de recondicionamento, manutenção ou reparação que resultem em modificações físicas de produtos com elementos digitais já colocados no mercado não constituem necessariamente modificações substanciais. Por conseguinte, deve ser realizada uma avaliação caso a caso, a fim de determinar se essa modificação física afeta a conformidade do produto com elementos digitais com os requisitos essenciais constantes da parte I do anexo I, ou se resulta numa alteração da finalidade prevista do produto abrangida pela avaliação dos riscos de cibersegurança.

95. A substituição de peças defeituosas ou de elementos gastos por peças com melhor desempenho (por exemplo, devido ao progresso técnico ou ao facto de a peça antiga já não ser produzida) não desencadeia, por si só, uma modificação substancial do produto com elementos digitais reparado. Só assim é se a alteração do desempenho ou do modo de funcionamento do produto com elementos digitais reparado i) afetar a sua conformidade com os requisitos essenciais ou ii) resultar numa alteração da finalidade prevista que não foi abrangida pela avaliação dos riscos.

Exemplo 35: o fabricante de um servidor informático realiza uma operação de reparação, substituindo uma RAM defeituosa por uma RAM nova com melhor desempenho. A conformidade do servidor com os requisitos essenciais não é afetada. O servidor tem um melhor desempenho, mas o seu novo desempenho mantém-se dentro da utilização prevista do mesmo, conforme tida em conta na avaliação dos riscos de cibersegurança. O servidor informático não é considerado substancialmente modificado.

4.2. **Peças sobresselentes**

96. O artigo 2.º, n.º 6, do Regulamento de Ciber-Resiliência estabelece que as peças sobresselentes destinadas a substituir componentes idênticos e fabricadas de acordo com as mesmas especificações que esses componentes não estão sujeitas ao Regulamento de Ciber-Resiliência. O considerando 29 estabelece ainda que a isenção abrange tanto as peças sobresselentes de produtos com elementos digitais disponibilizados antes do início da aplicação do Regulamento de Ciber-Resiliência como as peças sobresselentes que já tenham sido sujeitas a um procedimento de avaliação da conformidade, nos termos do regulamento.

97. A isenção prevista no artigo 2.º, n.º 6, do Regulamento de Ciber-Resiliência deve ser entendida como aplicável apenas quando a peça sobresselente é especificamente fornecida para reparar ou prolongar a durabilidade de um produto com elementos digitais já colocado no mercado (antes ou depois de 11 de dezembro de 2027). Caso um produto com elementos digitais seja fornecido como um produto autónomo, sem qualquer ligação à manutenção ou reparação de um produto com elementos digitais preexistente, é colocado no mercado na aceção do Regulamento de Ciber-Resiliência e não deve ser considerado uma peça sobresselente abrangida pelo âmbito de aplicação do artigo 2.º, n.º 6. A finalidade de manutenção ou reparação deverá ser evidente a partir do contexto do fornecimento, por exemplo através da identificação do produto com elementos digitais ou da família de produtos na encomenda ou oferta comercial, ou através do fornecimento por meio de canais de pós-venda ou de serviço. Os elementos de prova para este efeito também devem ser mantidos à disposição das autoridades de fiscalização do mercado. O facto de um produto com elementos digitais poder ser tecnicamente utilizado para substituir um componente não é, por si só, suficiente para o incluir no âmbito de aplicação da isenção na ausência desses elementos.

98. Por conseguinte, se uma peça sobresselente for idêntica a um componente já incluído num produto com elementos digitais colocado no mercado antes da data de aplicação do Regulamento de Ciber-Resiliência, ou que tenha sido colocado no mercado em conformidade com o referido regulamento, essa peça sobresselente não está, ela própria, sujeita ao Regulamento de Ciber-Resiliência.

99. A avaliação para determinar se uma peça sobresselente deve ser considerada idêntica a um componente deve centrar-se no seu papel funcional no produto com elementos digitais e nas características que possam ser pertinentes para a cibersegurança. Embora seja sempre necessária uma avaliação caso a caso, as diferenças que não afetem as características de segurança ou o perfil de risco de cibersegurança do componente não impedem, por si só, que essa peça sobresselente seja abrangida pelo âmbito de aplicação do artigo 2.º, n.º 6, do Regulamento de Ciber-Resiliência.

100. Em contrapartida, as diferenças nas características pertinentes para a cibersegurança do componente, como algoritmos, protocolos, mecanismos criptográficos, funcionalidades de controlo de acesso ou outras características pertinentes para a segurança, podem significar que a nova peça não pode ser considerada idêntica ao componente que se destina a substituir.

101. Se uma peça sobresselente não for idêntica ao componente original, essa peça sobresselente constitui um produto com elementos digitais em si mesma e está, por conseguinte, sujeita ao Regulamento de Ciber-Resiliência. Nesses casos, a conformidade com os requisitos essenciais deve ser avaliada à luz da finalidade prevista do componente de substituição. De particular pertinência é a função do componente de substituição de assegurar a compatibilidade ou interoperabilidade com um produto com elementos digitais existente, incluindo quando este é um produto com elementos digitais colocado no mercado antes do início da aplicação do Regulamento de Ciber-Resiliência. Caso determinados requisitos essenciais não possam ser razoavelmente cumpridos devido a essa finalidade prevista ou a condicionalismos técnicos, o fabricante deve refletir este facto na avaliação dos riscos de cibersegurança e aplicar medidas alternativas ou compensatórias de atenuação dos riscos adequadas, a fim de não comprometer a segurança do produto com elementos digitais. Conforme referido na secção *2.6 Sistemas complexos*, tanto a documentação técnica como as informações e instruções destinadas ao utilizador desempenham um papel fundamental na descrição transparente dos condicionalismos identificados, dos riscos de cibersegurança conexos e das medidas de atenuação dos riscos aplicadas. Como explicado na secção *4.1 Reparações físicas*, a substituição de peças defeituosas ou elementos gastos por peças com melhor desempenho não desencadeia, por si só, uma modificação substancial do produto com elementos digitais reparado.

Exemplo 36: um fabricante colocou controladores conectados no mercado da UE. Num caso, o controlador foi colocado no mercado em 2026, antes da data de aplicação do Regulamento de Ciber-Resiliência. Noutro caso, o controlador foi colocado no mercado em 2028, cumprindo o Regulamento de Ciber-Resiliência. Em 2028, um módulo de comunicação digital em ambos os tipos de controladores falhou. O fabricante fornece, como peça sobresselente, um módulo de substituição idêntico e fabricado de acordo com as mesmas especificações que o original.

Em ambos os casos, o módulo de substituição é abrangido pelo âmbito de aplicação da isenção prevista no artigo 2.º, n.º 6. A peça sobresselente não está, em si mesma, sujeita ao Regulamento de Ciber-Resiliência, apesar de ser um produto com elementos digitais, uma vez que substitui um componente idêntico num produto com elementos digitais. A reparação não constitui uma modificação substancial do produto com elementos digitais.

Exemplo 37: um fabricante colocou um controlador industrial conectado no mercado da UE em 2026, antes da data de aplicação do Regulamento de Ciber-Resiliência. Em 2028, um circuito integrado de comunicação existente nesse controlador falhou. Uma vez que o fabricante já não fabrica esse circuito integrado, fornece, como peça sobresselente, um circuito integrado mais recente com uma funcionalidade equivalente, mas com uma aplicação criptográfica diferente e um mecanismo de arranque seguro atualizado, a fim de manter a compatibilidade e o funcionamento contínuo.

Neste caso, o circuito integrado de substituição não pode ser considerado idêntico, pois as diferenças na aplicação criptográfica e no mecanismo de arranque seguro afetam as propriedades de cibersegurança do circuito integrado. Por conseguinte, não beneficia da isenção prevista no artigo 2.º, n.º 6, e constitui um produto com elementos digitais sujeito ao Regulamento de Ciber--Resiliência. A conformidade da peça de substituição deve ser avaliada à luz da sua finalidade prevista, incluindo o seu papel na garantia da interoperabilidade com o produto com elementos digitais colocado no mercado antes do início da aplicação do Regulamento de Ciber-Resiliência.

Exemplo 38: em 2028, um fabricante coloca no mercado um controlador de edifício inteligente, cumprindo o Regulamento de Ciber-Resiliência. Em 2029, o módulo sem fios desse controlador falhou. Uma vez que o fabricante já não fabrica esse módulo, fornece, como peça sobresselente, um novo módulo que desempenha a mesma função utilizando os mesmos protocolos de comunicação e mecanismos de segurança, mas que se baseia num conjunto de circuitos integrados diferente e dispõe de firmware *atualizado que não altera características que possam ser pertinentes para a cibersegurança.*

Neste caso, o módulo de substituição pode ser considerado idêntico. Por conseguinte, o módulo beneficia da isenção prevista no artigo 2.º, n.º 6, e não está sujeito ao Regulamento de Ciber-Resiliência.

102. A isenção para as peças sobresselentes aplica-se independentemente de a peça sobresselente substituir um componente de um produto com elementos digitais ou de substituir um produto com elementos digitais completo que, por sua vez, faça parte de um produto mais vasto, incluindo nos casos em que esse produto com elementos digitais mais vasto seja composto por vários componentes integrados, desde que a peça de substituição seja especificamente fornecida como peça sobresselente, conforme explicado nos números anteriores.

Exemplo 39: em 2027, um fabricante coloca no mercado um sistema de automatização industrial que incorpora um controlador lógico programável (PLC, do inglês programmable logic controller*) como um dos seus componentes. Em 2031, a unidade central de processamento (CPU, do inglês* central processing unit*) do PLC falhou. O fabricante disponibiliza duas opções de reparação: i) o fornecimento de uma CPU de substituição, que pode ser considerada idêntica à CPU originalmente instalada, ou ii) o fornecimento de um PLC de substituição completo, que pode ser considerado idêntico ao PLC originalmente instalado. Em cada caso, a substituição é fornecida através do canal de serviço pós-venda do fabricante, como peça sobresselente, e o sistema de automatização industrial a que a substituição se destina é claramente identificado. Em ambos os casos, a substituição é abrangida pelo âmbito de aplicação da isenção prevista no artigo 2.º, n.º 6, quer diga respeito a um componente do PLC, quer ao PLC no seu todo.*

4.3. **Atualizações de *software* como modificações substanciais**

103. O desenvolvimento de *software* é de natureza iterativa, sendo os produtos de *software* com elementos digitais já colocados no mercado frequente e continuamente atualizados. Neste contexto, é útil facultar mais orientações para determinar quando o *software* deve ser considerado substancialmente modificado. Essas orientações destinam-se, em especial, a ajudar os fabricantes de produtos de *software* com elementos digitais que introduzem alterações nos seus próprios produtos a determinar se essas alterações constituem uma modificação substancial.

104. O considerando 39 indica que um produto com elementos digitais é substancialmente modificado se uma alteração afetar o nível de risco de cibersegurança e se o fabricante não tiver tido esse risco alterado ou adicional em conta na sua avaliação dos riscos e, consequentemente, na sua aplicação dos requisitos essenciais. Por conseguinte, um fabricante deve avaliar, caso a caso, se uma atualização de *software* introduz riscos de cibersegurança novos ou acrescidos e se esses riscos já foram abordados na sua avaliação dos riscos.

105. Caso um fabricante introduza novas funcionalidades num produto com elementos digitais que resultem numa alteração da finalidade prevista do produto no seu todo, é provável que o fabricante não tenha tido em conta essas alterações na sua avaliação dos riscos. Em tais circunstâncias, a alteração seria geralmente considerada uma modificação substancial.

Exemplo 40: um fabricante coloca no mercado um painel que recolhe dados de máquinas e apresenta tendências e alertas, sem ter capacidade para controlar essas máquinas. Posteriormente, o fabricante desenvolve uma nova versão desse painel, introduzindo funcionalidades que lhe permitem controlar as máquinas, nomeadamente ao ajustar os parâmetros operacionais e reiniciar as máquinas em condições de falha. Em resultado destas alterações, a finalidade prevista do painel evoluiu para além do previsto na avaliação dos riscos, passando de uma ferramenta de conhecimento situacional para um produto com elementos digitais destinado a exercer controlo operacional sobre outros dispositivos. Por conseguinte, o painel foi substancialmente modificado.

Exemplo 41: um fabricante coloca no mercado uma aplicação informática de consumo destinada a organizar e apresentar dados pessoais, como mensagens de correio eletrónico, outras mensagens, ou documentos, e a apoiar funções básicas de pesquisa e filtragem. Posteriormente, o fabricante introduz uma atualização que permite à aplicação analisar automaticamente o conteúdo do utilizador, a fim de gerar perfis comportamentais e tomar decisões automatizadas que afetam a definição de prioridades, a supressão ou a recomendação de conteúdos sem intervenção do utilizador. Em resultado desta alteração, a finalidade prevista do software *passa de uma ferramenta de gestão da informação controlada pelo utilizador para um sistema automatizado de tomada de decisões, o que não estava previsto na avaliação dos riscos. Por conseguinte, a aplicação foi substancialmente modificada.*

106. Ao mesmo tempo, no entanto, é possível um fabricante introduzir progressivamente novas funcionalidades já incluídas na sua avaliação dos riscos ou que, por si só, não alterem o perfil de risco de cibersegurança do produto com elementos digitais. Pode ser o caso, por exemplo, se o fabricante tiver antecipado o desenvolvimento dessas funcionalidades, já tiver descrito e avaliado os riscos associados e tiver aplicado medidas de atenuação adequadas para assegurar a conformidade contínua com os requisitos essenciais. Também pode ser o caso quando as novas funcionalidades não implementam alterações que introduzam riscos novos ou acrescidos. Por conseguinte, as atualizações desta natureza não devem ser consideradas modificações substanciais, pois não aumentam o risco de cibersegurança e, consequentemente, não alteram a aplicação dos requisitos essenciais.

Exemplo 42: uma aplicação de mensagens é inicialmente lançada com uma funcionalidade limitada ao envio de mensagens «um para um». A avaliação dos riscos que o fabricante efetua abrange a introdução posterior de mensagens de grupo, incluindo, por exemplo, o aumento da complexidade do encaminhamento das mensagens. Numa atualização subsequente, o fabricante adiciona uma funcionalidade de conversa em grupo, juntamente com controlos de administrador e ferramentas de moderação já previstas e avaliadas na conceção original. A atualização implementa funcionalidades que se inserem no âmbito da finalidade prevista inicial e da avaliação dos riscos. Por conseguinte, a aplicação de mensagens não foi substancialmente modificada.

Exemplo 43: é colocado no mercado um sistema de monitorização da produção com painéis apenas de leitura ativados, existindo funcionalidades de controlo automático na arquitetura do sistema, mas estas continuam desativadas. A avaliação dos riscos do fabricante abrange explicitamente a futura ativação dos circuitos de controlo automatizados, incluindo os riscos de cibersegurança associados ao controlo em circuito fechado, bem como salvaguardas, como mecanismos de neutralização do operador e estados de segurança à prova de falhas. Numa atualização posterior, o fabricante ativa as funcionalidades de controlo automatizado e as salvaguardas, tal como inicialmente avaliadas. Por conseguinte, o sistema de monitorização da produção não foi substancialmente modificado.

107. Em contrapartida, mesmo novas funcionalidades limitadas ou aparentemente menores podem introduzir riscos de cibersegurança significativos que afetam o cumprimento dos requisitos essenciais. Por conseguinte, a avaliação da modificação substancial não deve basear-se na escala ou complexidade da alteração, mas sim no seu potencial impacto negativo no perfil de risco de cibersegurança do produto com elementos digitais e, consequentemente, na aplicação dos requisitos essenciais.

Exemplo 44: um fabricante introduz uma atualização numa aplicação informática que adiciona uma funcionalidade «lembrar-se de mim» ou de início de sessão persistente que armazena localmente fichas de autenticação para maior comodidade do utilizador. Embora a funcionalidade possua um âmbito limitado, introduz novos riscos relacionados com o roubo de fichas, o acesso não autorizado e o sequestro de sessão que não foram tidos em conta na avaliação dos riscos. Por conseguinte, a atualização afeta o cumprimento dos requisitos essenciais. A aplicação informática foi substancialmente modificada.

Exemplo 45: um fabricante adiciona uma nova funcionalidade de registo e diagnóstico a um produto de software *existente com elementos digitais, ativando a exportação de registos pormenorizados do sistema para efeitos de resolução de problemas. Embora a funcionalidade se afigure menor, resulta na recolha e armazenamento de dados operacionais sensíveis num formato não cifrado, introduzindo riscos de exposição dos dados que não foram previamente avaliados ou atenuados. Por conseguinte, a alteração pode ter um impacto significativo no perfil de risco de cibersegurança do produto com elementos digitais. O produto de* software *com elementos digitais foi substancialmente modificado.*

108. Em conformidade com o considerando 39 do Regulamento de Ciber-Resiliência, as atualizações de segurança não devem, de um modo geral, ser consideradas modificações substanciais, pois o seu principal objetivo consiste em reduzir o nível de risco de cibersegurança associado ao produto com elementos digitais. Uma atualização de segurança que não modifique a finalidade prevista desse produto e não introduza novos riscos de cibersegurança não deverá, por conseguinte, ser considerada uma modificação substancial, mesmo que essa atualização possa introduzir alterações técnicas significativas. Inclui-se casos em que determinadas funcionalidades são modificadas ou condicionadas exclusivamente com o objetivo de atenuar as vulnerabilidades identificadas e assegurar o cumprimento permanente dos requisitos essenciais.

Exemplo 46: um fabricante implanta uma atualização de segurança para dar resposta a uma vulnerabilidade na base de códigos de um produto com elementos digitais, corrigindo um erro de validação da entrada de dados que possa conduzir a um transbordamento de buffer *ou uma falha lógica que permita contornar a autenticação através de uma validação incorreta da ficha de sessão. A atualização modifica a implementação interna do* software *sem afetar a finalidade prevista desse produto nem introduzir uma nova exposição. Essa atualização destina-se exclusivamente a reduzir o risco de cibersegurança. A atualização de segurança não deve ser considerada uma modificação substancial.*

Exemplo 47: um fabricante introduz uma atualização de segurança que reforça as configurações de segurança existentes, como o reforço das regras da barreira de segurança, a desativação de portas de rede não utilizadas, a alteração das políticas de palavra-passe do administrador predefinidas ou a obrigatoriedade de autenticação multifatores, caso essa funcionalidade já estivesse disponível ou prevista. Embora a atualização possa afetar a forma como os utilizadores configuram ou acedem ao produto com elementos digitais, não altera a sua finalidade prevista e serve apenas para reforçar a sua postura de segurança. A atualização de segurança não deve ser considerada uma modificação substancial.

Exemplo 48: um fabricante coloca no mercado um produto de software *com elementos digitais que protege as comunicações utilizando um quadro de cifragem configurável que suporta múltiplos algoritmos criptográficos e dimensões de chaves, conforme descrito na documentação técnica e na avaliação dos riscos do produto. A avaliação dos riscos abrange todas as opções criptográficas fornecidas no produto com elementos digitais e prevê a futura depreciação de determinados algoritmos. A avaliação dos riscos inclui igualmente medidas de atenuação, como a agilidade criptográfica, a gestão interna das chaves e os ensaios de compatibilidade. Em resposta às orientações criptográficas emergentes, o fabricante implanta uma atualização de segurança que desativa um algoritmo obsoleto e ativa uma alternativa mais forte e já apoiada, sem introduzir novas dependências externas nem alterar os fluxos de dados. Uma vez que a atualização aplica uma medida de segurança prevista e avaliada como parte da conceção original e não introduz novos riscos de cibersegurança, a atualização de segurança não deve ser considerada uma modificação substancial.*

109. Em contrapartida, uma atualização de segurança pode ser considerada uma modificação substancial se, não obstante o seu objetivo de segurança, a atualização resultar na modificação da finalidade prevista do produto com elementos digitais para além do inicialmente previsto ou introduzir riscos de cibersegurança novos ou acrescidos. Pode ser o caso, por exemplo, quando uma atualização altera substancialmente os limites ou a estrutura de dependência desse produto de uma forma não prevista na avaliação dos riscos, por exemplo, alterando substancialmente os fluxos de dados ou adicionando novas interfaces acessíveis do exterior.

Exemplo 49: um fabricante coloca no mercado um produto de software *com elementos digitais destinado a fornecer cifragem local de ficheiros para dados armazenados num dispositivo de um utilizador, permitindo aos utilizadores cifrar e decifrar ficheiros a pedido. Na sequência da descoberta de uma vulnerabilidade no fluxo de trabalho da cifragem, o fabricante implanta uma atualização de segurança que elimina a funcionalidade local de cifragem e, em vez disso, exige que todos os ficheiros sejam carregados, armazenados e tratados por um serviço remoto de cifragem operado pelo fabricante. Em resultado desta alteração, o produto com elementos digitais deixou de realizar a cifragem local inicialmente prevista, funcionando, em vez disso, como um serviço de cifragem e tratamento de dados remoto. Embora a atualização seja introduzida por razões de segurança, altera fundamentalmente a finalidade prevista desse produto de uma forma não prevista na avaliação dos riscos e, por conseguinte, pode ser considerada uma modificação substancial.*

Exemplo 50: um fabricante coloca no mercado um produto de software *com elementos digitais que recorre a um protocolo de cifragem estabelecido e a um ciclo de vida essencial gerido internamente para garantir a segurança das comunicações entre os componentes do produto com elementos digitais. Em resposta a deficiências criptográficas recentemente identificadas, o fabricante introduz uma atualização de segurança que substitui o mecanismo de cifragem existente por um protocolo diferente que exige a utilização de um serviço externo de gestão de chaves operado por um terceiro. Em resultado desta alteração, as dependências e os fluxos de dados do produto com elementos digitais são substancialmente alterados, introduzindo novas interfaces externas e o recurso a serviços de terceiros que não foram tidos em conta na avaliação dos riscos. Embora a atualização seja orientada para a segurança, introduz novos riscos de cibersegurança e, por conseguinte, pode ser considerada uma modificação substancial.*

110. Conforme referido no ponto 104 *supra*, a questão de saber se uma atualização de *software* constitui uma modificação substancial deve ser avaliada caso a caso. Ao realizar essa avaliação, os fabricantes podem ter em conta, de forma não exaustiva, se a atualização do *software*:

a) Introduz novos vetores de ameaça, como interfaces adicionais, canais de comunicação, ambientes de execução ou dependências externas através dos quais se possam materializar ameaças;

b) Permite novos cenários de ataque, incluindo, por exemplo, novas formas de o acesso não autorizado, a manipulação, a interferência ou a utilização indevida do produto com elementos digitais ou dos dados por ele tratados poderem ocorrer de forma plausível;

c) Altera a probabilidade de cenários de ataque previamente identificados, por exemplo, reduzindo o esforço ou os conhecimentos especializados necessários para os explorar, aumentando a exposição a intervenientes não fiáveis ou enfraquecendo as salvaguardas existentes;

d) Altera o potencial impacto de cenários de ataque previamente identificados, incluindo, por exemplo, o âmbito dos dados ou funções afetados, a gravidade das consequências operacionais, económicas ou de segurança, ou a capacidade de detetar, conter ou recuperar de um incidente.

111. Em alguns casos, uma atualização de *software* não introduz novos vetores de ameaça, não permite novos cenários de ataque e não altera substancialmente a probabilidade ou o impacto de cenários de ataque previamente identificados. Tal pode indicar que a atualização não introduz riscos de cibersegurança novos ou acrescidos, desde que os pressupostos e as medidas de atenuação utilizados na avaliação dos riscos permaneçam válidos e eficazes. Por conseguinte, é provável que a atualização não seja considerada uma modificação substancial.

112. Em contrapartida, uma atualização de *software* pode introduzir novos vetores de ameaça, permitir novos cenários de ataque ou alterar substancialmente a probabilidade ou o impacto de cenários de ataque existentes. Nesses casos, o fabricante deve reavaliar os riscos de cibersegurança do produto com elementos digitais e determinar se os requisitos essenciais continuam a ser cumpridos, nomeadamente se a atualização introduz riscos novos ou acrescidos não previstos na avaliação dos riscos.

113. A questão de saber se uma atualização de *software* pode ser considerada uma modificação substancial é pertinente para determinar se são aplicáveis determinadas obrigações por força do Regulamento de Ciber-Resiliência, conforme estabelecido no ponto 91. Todavia, independentemente dessa qualificação, os fabricantes continuam a ser responsáveis por garantir a segurança das atualizações de *software* e do seu produto com elementos digitais durante o respetivo período de apoio, em conformidade com os requisitos de tratamento de vulnerabilidades estabelecidos na parte II do anexo I do Regulamento de Ciber-Resiliência. Além disso, independentemente de as atualizações de *software* serem ou não consideradas modificações substanciais, os fabricantes são obrigados a manter a avaliação dos riscos e a documentação técnica exatas, completas e continuamente atualizadas, por força do artigo 13.º, n.º 7, e do artigo 31.º, n.º 2.

4.4. **Consequências de uma modificação substancial**

114. As consequências de uma modificação substancial efetuada por um interveniente que não seja o fabricante original de um produto com elementos digitais já colocado no mercado são abordadas nos artigos 21.º e 22.º do Regulamento de Ciber-Resiliência. O artigo 21.º diz respeito aos importadores e distribuidores, ao passo que o artigo 22.º diz respeito a qualquer pessoa singular ou coletiva que não seja o fabricante, importador ou distribuidor.

115. Se a modificação substancial for efetuada pelo fabricante original do produto com elementos digitais, as consequências decorrem do conceito geralmente estabelecido de modificação substancial a que se refere o considerando 41 do Regulamento de Ciber-Resiliência e são aprofundadas na secção 2.1 do Guia Azul. Esta secção indica que um produto que tenha sido objeto de alterações significativas ou de uma revisão após a sua colocação no mercado deve ser considerado um produto novo caso o seu desempenho, a sua finalidade ou o seu tipo de origem tenha sido modificado, a natureza do perigo tenha mudado ou o nível de risco tenha aumentado e o produto com elementos digitais seja disponibilizado no mercado.

116. Por conseguinte, a consequência geralmente estabelecida é que, caso uma modificação de um produto com elementos digitais seja considerada uma modificação substancial e o produto com elementos digitais modificado seja disponibilizado no mercado, deve ser tratado como um novo produto com elementos digitais para efeitos do Regulamento de Ciber-Resiliência. Como resultado, o ato de disponibilizar no mercado o produto substancialmente modificado constitui uma nova colocação no mercado. Tal aplica-se quer a modificação substancial seja efetuada pelo fabricante original quer por outra pessoa. A fim de assegurar que o Regulamento de Ciber-Resiliência é aplicado de modo uniforme e proporcionado nas diferentes categorias de intervenientes que podem efetuar uma modificação substancial, as subsecções que se seguem abordam as obrigações resultantes da pessoa que efetua a modificação substancial quando o produto com elementos digitais substancialmente modificado é colocado no mercado. As consequências para o período de apoio do produto com elementos digitais são abordadas na secção *5 Período de* apoio.

4.4.1. *Modificações substanciais efetuadas por outra pessoa que não o fabricante original*

117. Em conformidade com os artigos 21.º e 22.º, caso uma modificação substancial de um produto com elementos digitais já colocado no mercado seja efetuada por uma pessoa singular ou coletiva que não seja o fabricante do produto com elementos digitais, a pessoa que efetua a modificação substancial e disponibiliza no mercado o produto com elementos digitais modificado deve ser considerada o fabricante do produto com elementos digitais modificado, independentemente de essa pessoa ter estado envolvida ou não na conceção ou na colocação no mercado inicial desse produto.

118. O artigo 22.º esclarece ainda que a pessoa que efetua a modificação está sujeita às obrigações estabelecidas nos artigos 13.º e 14.º apenas no que diz respeito à parte do produto com elementos digitais afetada pela modificação substancial, se essa modificação não afetar a cibersegurança do produto com elementos digitais no seu todo.

119. Caso uma modificação substancial afete a conformidade com os requisitos essenciais, mas não afete negativamente a cibersegurança do produto com elementos digitais no seu todo, a pessoa que efetua a modificação está sujeita aos artigos 13.º (incluindo a obrigação de assegurar o cumprimento dos requisitos essenciais e de realizar um procedimento de avaliação da conformidade) e 14.º (obrigações em matéria de comunicação de informações) apenas em relação à parte do produto com elementos digitais que tenha sido substancialmente modificada ([16]). Além disso, as obrigações impostas ao fabricante original por força do Regulamento de Ciber-Resiliência continuam a aplicar-se ao produto original com elementos digitais colocado no mercado, assegurando a continuidade do tratamento de vulnerabilidades e a conformidade das partes inalteradas.

120. Não deve confundir-se um caso de modificação substancial com casos de integração, em que uma pessoa instala componentes (incluindo, se for caso disso, modificando-os) num novo produto com elementos digitais que ela própria coloca no mercado. Nesses casos, o responsável pela integração não está a modificar um produto com elementos digitais já colocado no mercado por outro fabricante; está, isso sim, a colocar no mercado um novo produto com elementos digitais da sua própria conceção. O responsável pela integração é o fabricante desse novo produto com elementos digitais para efeitos do Regulamento de Ciber-Resiliência e é obrigado a cumprir o regulamento na sua totalidade no que diz respeito ao produto com elementos digitais no seu todo. Se o fabricante integrar componentes sujeitos ao Regulamento de Ciber-Resiliência, pode recorrer às atividades de conformidade dos fabricantes dos componentes para facilitar a sua própria conformidade com o Regulamento de Ciber--Resiliência.

Exemplo 51: uma empresa compra módulos de microcontroladores e componentes de conectividade prontos a utilizar a fornecedores terceiros, desenvolve firmware *proprietário e um pacote de sensores, e instala-os num produto de monitorização agrícola conectado com elementos digitais que coloca no mercado em seu próprio nome. Embora a empresa tenha modificado os módulos dos microcontroladores subjacentes e os tenha combinado com outros componentes, não está a modificar substancialmente um produto com elementos digitais já colocado no mercado; está, isso sim, a colocar no mercado um novo produto com elementos digitais. Para efeitos do Regulamento de Ciber-Resiliência, a empresa é o fabricante do monitor agrícola e é obrigada a cumprir o regulamento no que diz respeito ao monitor agrícola no seu todo.*

([16]) Em consonância com a secção 2.1 do Guia Azul, «[n]ão é necessário repetir os ensaios nem produzir nova documentação em relação a aspetos não afetados pela alteração. Cabe à pessoa singular ou coletiva que efetua as alterações ou manda efetuar as alterações no produto demonstrar que nem todos os elementos da documentação técnica necessitam de ser atualizados. Essa pessoa singular ou coletiva é responsável pela conformidade do produto modificado e pela elaboração de uma declaração de conformidade, mesmo que utilize ensaios e documentação técnica existentes».

121. Caso uma modificação substancial efetuada por uma pessoa que não seja o fabricante original afete negativamente a cibersegurança do produto com elementos digitais no seu todo, por exemplo porque a modificação deixou de ser direcionada ou limitada a um componente ou subsistema específico, o produto com elementos digitais modificado disponibilizado no mercado deverá ser tratado como um novo produto com elementos digitais sujeito ao Regulamento de Ciber-Resiliência na sua totalidade. Nesses casos, o perfil global de risco de cibersegurança desse produto alterou-se e a modificação não pode ser avaliada sem ter em conta o produto com elementos digitais no seu todo. A pessoa que efetua a modificação está sujeita às obrigações aplicáveis ao fabricante estabelecidas nos artigos 13.º e 14.º no que diz respeito ao produto com elementos digitais modificado no seu todo.

4.4.2. *Modificações substanciais efetuadas pelo fabricante original*

122. Caso a modificação substancial seja efetuada pelo fabricante original, nomeadamente no contexto do desenvolvimento iterativo de produtos de *software* com elementos digitais, esse fabricante continua a ser o fabricante para efeitos do Regulamento de Ciber-Resiliência. Todavia, deve considerar-se que o produto com elementos digitais substancialmente modificado foi recentemente colocado no mercado.

123. Em conformidade com a secção 2.1 do Guia Azul, o fabricante original que coloca no mercado o produto com elementos digitais substancialmente modificado pode reutilizar a documentação e os ensaios existentes para aspetos do produto com elementos digitais que não sejam afetados pela modificação substancial. Em especial, se o fabricante colocar no mercado versões substancialmente modificadas do mesmo produto com elementos digitais, o procedimento de avaliação da conformidade deve centrar-se nas partes substancialmente modificadas do produto com elementos digitais. Do mesmo modo, quando é efetuada uma avaliação da conformidade por terceiros, o organismo de avaliação da conformidade deve centrar a sua avaliação nas partes substancialmente modificadas. Para as partes inalteradas do produto com elementos digitais, pode reutilizar a documentação e os resultados de ensaios existentes.

124. As considerações de proporcionalidade estabelecidas na subsecção anterior aplicam-se igualmente às modificações substanciais efetuadas pelo fabricante original de um produto com elementos digitais colocado no mercado antes de 11 de dezembro de 2027. Essa modificação substancial efetuada pelo fabricante original não exige, por si só, que o fabricante faça com que todo o produto com elementos digitais colocado no mercado antes dessa data fique plenamente conforme com o Regulamento de Ciber-Resiliência, a menos que a modificação afete negativamente a cibersegurança do produto com elementos digitais no seu todo. Se a modificação não afetar a cibersegurança do produto com elementos digitais no seu todo, as obrigações aplicáveis ao fabricante original no que diz respeito à modificação deverão limitar-se às partes substancialmente modificadas.

5. **PERÍODO DE APOIO**

125. O artigo 13.º, n.º 8, do Regulamento de Ciber-Resiliência exige que os fabricantes determinem o período de apoio durante o qual as vulnerabilidades do produto com elementos digitais, incluindo dos seus componentes, são tratadas de forma eficaz e em conformidade com os requisitos essenciais constantes da parte II do anexo I. O período de apoio reflete o intervalo de tempo durante o qual se prevê que o produto com elementos digitais seja utilizado (o tempo de utilização previsto) e deve ser determinado à luz dos critérios estabelecidos no artigo 13.º, n.º 8, em especial as expectativas razoáveis dos utilizadores, a natureza do produto com elementos digitais, incluindo a sua finalidade prevista, bem como a legislação pertinente da União que determina a vida útil dos produtos com elementos digitais ([17]). De um modo geral, esses critérios devem ser tidos em conta de forma a garantir proporcionalidade na determinação do período de apoio.

([17]) É possível ter em conta critérios adicionais, em conformidade com o artigo 13.º, n.º 8, nomeadamente 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) previsto no Regulamento de Ciber-Resiliência e pela Comissão.

126. O artigo 13.º, n.º 8, exige ainda que o período de apoio seja de, pelo menos, cinco anos, a menos que se preveja que o produto com elementos digitais seja utilizado durante menos de cinco anos, caso em que o período de apoio deve corresponder ao tempo de utilização previsto. Por conseguinte, o período mínimo de apoio funciona apenas como uma salvaguarda, assegurando que as vulnerabilidades são tratadas durante um período suficientemente longo, permitindo simultaneamente que os fabricantes tenham em conta produtos com elementos digitais com tempos de utilização previstos verdadeiramente mais curtos. O considerando 60 faculta mais orientações a este respeito, esclarecendo que sempre que seja razoável esperar que os produtos com elementos digitais sejam utilizados durante um período superior a cinco anos, dever-se-á assegurar períodos de apoio mais longos em conformidade. Por conseguinte, não deve considerar-se que um período de apoio de cinco anos é uma predefinição para todos os produtos com elementos digitais. Em vez disso, o fabricante deve determinar o período de apoio adequado à luz dos critérios referidos no artigo 13.º, n.º 8.

127. O artigo 13.º, n.º 19, exige que os fabricantes indiquem no momento da compra, de forma clara e compreensível, a data final do período de apoio (pelo menos o mês e o ano). Exige igualmente que, sempre que seja tecnicamente viável tendo em conta a natureza do produto com elementos digitais, os fabricantes apresentem uma notificação aos utilizadores após o fim do período de apoio. Esta obrigação destina-se a proporcionar transparência aos utilizadores no que diz respeito à duração prevista do apoio no domínio da segurança.

128. No caso de produtos de *software* com elementos digitais, que são frequentemente desenvolvidos e lançados iterativamente e em que versões substancialmente modificadas podem ser colocadas no mercado com frequência ao longo do tempo, deve entender-se o período de apoio à luz deste modelo de desenvolvimento. Cada versão substancialmente modificada de um produto de *software* com elementos digitais colocado no mercado tem de ter um período de apoio declarado que cumpra o disposto no artigo 13.º, n.º 8. Tal inclui o período mínimo de apoio de, pelo menos, cinco anos, salvo se o tempo de utilização previsto dessa versão for comprovadamente mais curto, conforme também clarificado no considerando 60. A secção *5.1 Modificações substanciais e período de apoio* esclarece ainda que, caso a modificação substancial não conduza a alterações dos fatores que determinaram originalmente o tempo de utilização previsto do produto com elementos digitais, o período de apoio original não é afetado (ou seja, incluindo nos casos em que o período de apoio remanescente é inferior a cinco anos).

129. O artigo 13.º, n.º 10, proporciona flexibilidade aos produtos de *software* com elementos digitais, permitindo que os fabricantes, em determinadas condições, assegurem o cumprimento do requisito de tratamento de vulnerabilidades estabelecido na parte II, ponto 2, do anexo I (o tratamento e a correção de vulnerabilidades), apenas para a última versão do produto de *software* com elementos digitais colocada no mercado. Tal é permitido quando os utilizadores de versões anteriormente colocadas no mercado têm acesso gratuito à última versão colocada no mercado e não incorrem em custos adicionais para ajustar o ambiente de *hardware* e *software* em que utilizam a versão original desse produto.

130. Para efeitos do artigo 13.º, n.º 10, deve interpretar-se o conceito de «custos adicionais» de forma prática e proporcionada, tendo em conta as práticas normais e previstas em matéria de manutenção e funcionamento do *software*. Não abrange esforços operacionais razoáveis inerentes à aplicação de atualizações de *software* ou à manutenção de um ambiente operacional seguro, como tempo de trabalho, ensaios de rotina, ajustamentos da configuração ou atualizações das dependências de *software* subjacentes que sejam necessários para tratar de componentes em fim de vida ou vulnerabilidades de segurança conhecidas. Em contrapartida, os «custos adicionais» referem-se a encargos que vão além do que normalmente se pode esperar no contexto de atualizações de *software*, como aquisições obrigatórias de novo *hardware*, substituição de infraestruturas ou alterações fundamentais do ambiente operacional.

131. No caso de produtos de *software* com elementos digitais em constante evolução, os fabricantes podem colocar no mercado sucessivas versões substancialmente modificadas a intervalos relativamente curtos e esperar que os utilizadores as atualizem periodicamente. Nesses casos, o período de apoio declarado para cada versão substancialmente modificada deve cumprir o disposto no artigo 13.º, n.º 8, no momento da sua colocação no mercado. Por outras palavras, o fabricante deve declarar um novo período de apoio para essa versão substancialmente modificada. Todavia, os fabricantes podem invocar o artigo 13.º, n.º 10, para pôr termo ao tratamento e à correção de vulnerabilidades de versões anteriores quando for possível para os utilizadores atualizá-

las para uma versão posterior, a título gratuito e sem incorrer em custos adicionais, conforme referido *supra*, mesmo que tal resulte num período de apoio efetivo mais curto para essas versões anteriores ([18]). O fabricante continua sujeito aos outros requisitos de tratamento de vulnerabilidades previstos na parte II do anexo I, bem como às obrigações em matéria de comunicação de informações previstas no artigo 14.º. Conforme explicado no considerando 40, estes requisitos incluem, nomeadamente, para todas as versões substancialmente modificadas subsequentes do produto de *software* com elementos digitais colocado no mercado: i) manter uma política de divulgação coordenada de vulnerabilidades e ii) medidas para facilitar a partilha de informações sobre potenciais vulnerabilidades ([19]).

Exemplo 52: um fabricante coloca um modelo de telemóvel inteligente no mercado da UE e declara um período de apoio de X anos a contar da data de colocação no mercado, durante o qual disponibilizará atualizações de segurança para tratar de vulnerabilidades. Durante esse período, o fabricante lança atualizações periódicas do software *e versões substancialmente modificadas do sistema operativo, que os utilizadores podem instalar gratuitamente sem necessidade de novo* hardware.

Em conformidade com o artigo 13.º, n.º 10, o fabricante pode tratar e corrigir vulnerabilidades da versão mais recente do sistema operativo disponibilizada para esse modelo de telemóvel inteligente, desde que seja possível atualizar as versões anteriores gratuitamente e sem custos adicionais. Durante o período de apoio, o fabricante continua sujeito aos outros requisitos de tratamento de vulnerabilidades, como a divulgação coordenada de vulnerabilidades e medidas de partilha de informações.

Exemplo 53: um fabricante coloca no mercado um produto de software *empresarial com elementos digitais e lança, com intervalos de poucos meses, versões substancialmente modificadas que refletem melhorias de segurança, novas funcionalidades e compatibilidade com sistemas operativos e plataformas atualizados. Cada versão é colocada no mercado com um período de apoio declarado em conformidade com o artigo 13.º, n.º 8. O fabricante espera que os utilizadores procedam periodicamente à atualização no âmbito do funcionamento normal e faculta acesso gratuito à versão mais recente. A aplicação de atualizações pode exigir um esforço operacional razoável, como ensaios ou ajustamentos da configuração, mas não exige custos adicionais, como a aquisição de novo* hardware *ou alterações fundamentais das infraestruturas. Neste contexto, o fabricante pode invocar o artigo 13.º, n.º 10, para pôr termo ao tratamento e à correção de vulnerabilidades de versões anteriores assim que for possível para os utilizadores atualizá-las para a versão mais recente, continuando simultaneamente a cumprir os outros requisitos de tratamento de vulnerabilidades para todas as versões substancialmente modificadas subsequentes.*

5.1. **Modificações substanciais e período de apoio**

132. Conforme estabelecido na secção *4.4 Consequências de uma modificação substancial*, caso uma modificação de um produto com elementos digitais seja considerada uma modificação substancial e o produto com elementos digitais modificado seja disponibilizado no mercado, deve ser tratado como um novo produto para efeitos do Regulamento de Ciber-Resiliência, e o ato de disponibilizar no mercado o produto com elementos digitais substancialmente modificado constitui uma nova colocação no mercado. Por conseguinte, é útil clarificar o efeito desta nova colocação no mercado no período de apoio do produto com elementos digitais substancialmente modificado.

133. Deve determinar-se o período de apoio de um produto com elementos digitais substancialmente modificado por referência ao tempo de utilização previsto desse produto, à luz dos critérios estabelecidos no artigo 13.º, n.º 8, do Regulamento de Ciber-Resiliência. Por conseguinte, uma modificação substancial deve exigir uma reavaliação em função desses critérios, mas não resulta automaticamente na reinicialização do período de apoio, ou mesmo na sua prorrogação. A questão pertinente consiste em saber se a modificação substancial afeta os fatores que determinaram originalmente o tempo de utilização previsto desse produto e, por conseguinte, o período de apoio original.

([18]) Importa recordar que o artigo 13.º, n.º 19, exige que os fabricantes, sempre que seja tecnicamente viável tendo em conta a natureza do produto com elementos digitais, apresentem uma notificação aos utilizadores informando-os de que o seu produto com elementos digitais atingiu o fim do respetivo período de apoio. Por conseguinte, caso tenha sido posto termo ao tratamento e à correção de vulnerabilidades de versões anteriores, espera-se que os utilizadores que não tenham procedido à atualização para a versão mais recente sejam informados, se tal for tecnicamente viável.

([19]) Importa notar que, mesmo que os utilizadores possam proceder à atualização para a versão mais recente do *software* sem custos adicionais, os fabricantes continuam a poder optar por prosseguir o tratamento e a correção de vulnerabilidades em versões anteriores desse *software*, incluindo a título pago ou ao abrigo de outros acordos comerciais. O Regulamento de Ciber-Resiliência não exige que os fabricantes facultem, a título gratuito, atualizações de segurança para essas versões anteriores.

134. Caso a modificação substancial não afete esses fatores, os critérios estabelecidos no artigo 13.º, n.º 8, continuam a indicar o mesmo tempo de utilização previsto determinado originalmente, e o período de apoio do produto com elementos digitais modificado deve alinhar-se com o tempo de utilização remanescente previsto do produto tal como originalmente colocado no mercado. Habitualmente, tal será o caso quando o tempo de utilização previsto foi determinado principalmente por fatores que a modificação não altera, como a durabilidade física dos componentes de *hardware*, caso a modificação substancial diga apenas respeito à funcionalidade do *software* ou a serviços de retaguarda.

Exemplo 54: *um fabricante coloca no mercado um aspirador-robô com um tempo de utilização previsto de X anos, determinado com base na natureza do produto com elementos digitais, incluindo a durabilidade física e as características de desgaste dos componentes de* hardware*, bem como tendo em conta as expectativas razoáveis dos utilizadores quanto à vida útil desse produto. O fabricante estabelece um período de apoio de X anos. Após Y anos, o fabricante lança uma atualização do* software *que se qualifica como uma modificação substancial, adicionando novos modos de limpeza e funcionalidades de navegação. A atualização do* software *não afeta a durabilidade física do* hardware *e não altera as expectativas razoáveis dos utilizadores quanto à vida útil desse produto. Por conseguinte, os critérios constantes do artigo 13.º, n.º 8, continuam a indicar o mesmo tempo de utilização previsto. O período de apoio do produto com elementos digitais modificado está em consonância com o tempo de utilização remanescente previsto, conforme inicialmente determinado.*

Exemplo 55: um fabricante coloca no mercado um produto complexo de maquinaria industrial com elementos digitais, com uma retaguarda na nuvem que constitui uma solução de tratamento remoto de dados. O tempo de utilização previsto é de X anos, determinado à luz das expectativas razoáveis dos utilizadores e da natureza do produto com elementos digitais, como a durabilidade física do hardware *da maquinaria e o desgaste previsto. O período de apoio é definido em consonância com o tempo de utilização previsto de X anos. Após Y anos, o fabricante reformula a retaguarda na nuvem (a solução de tratamento remoto de dados), introduzindo novas IPA e fluxos de dados, de uma forma que se qualifica como uma modificação substancial do produto com elementos digitais, mas que não altera a natureza desse produto nem afeta as expectativas dos utilizadores. Por conseguinte, os critérios constantes do artigo 13.º, n.º 8, continuam a indicar o mesmo tempo de utilização previsto. O período de apoio do produto com elementos digitais modificado está em consonância com o tempo de utilização remanescente previsto, conforme inicialmente determinado.*

135. Caso a modificação substancial afete os fatores que determinaram originalmente o tempo de utilização previsto do produto com elementos digitais, o fabricante deve recalcular o período de apoio de modo a refletir o novo tempo de utilização previsto, aplicando os critérios constantes do artigo 13.º, n.º 8, em conformidade. Pode ser o caso, por exemplo, da revitalização de modificações do *hardware* que prolonguem a vida operacional desse produto, ou de uma reprogramação ou reescrita substancial do *software* de base desse produto que altere substancialmente o seu tempo de utilização previsto ([20]).

Exemplo 56: um fabricante coloca no mercado um controlador lógico programável (PLC) com um tempo de utilização previsto de X anos, determinado principalmente com base na natureza do produto com elementos digitais e na durabilidade do hardware *subjacente. O período de apoio é definido em conformidade. Vários anos após a colocação inicial no mercado, o fabricante efetua uma modificação substancial que consiste na substituição da plataforma computacional incorporada do PLC, incluindo o processador, a memória e o ambiente de* runtime*, por uma nova geração de componentes concebidos para um período de vida operacional significativamente mais longo. Em resultado da modificação, as expectativas razoáveis dos utilizadores e a natureza do produto com elementos digitais alteram-se: os utilizadores do PLC podem agora razoavelmente esperar que a utilização produtiva do PLC se prolongue para além do seu tempo de utilização originalmente previsto, apoiada pela nova plataforma computacional. Por conseguinte, os critérios constantes do artigo 13.º, n.º 8, indicam um período de utilização previsto mais longo e o fabricante recalcula o período de apoio para esse PLC específico em conformidade.*

6. **PRODUTOS IMPORTANTES E CRÍTICOS COM ELEMENTOS DIGITAIS**

136. O artigo 7.º, n.º 1, do Regulamento de Ciber-Resiliência estabelece que os produtos com elementos digitais cuja funcionalidade principal é a de uma categoria de produtos constante do anexo III do regulamento são considerados «produtos importantes com elementos digitais». O anexo III divide ainda os produtos importantes com elementos digitais nas classes I e II. Do mesmo modo, o artigo 8.º, n.º 1, estabelece que os produtos com elementos digitais cuja funcionalidade principal é a de uma categoria de produtos constante do anexo IV do Regulamento de Ciber-Resiliência são considerados «produtos críticos com elementos digitais» ([21]).

([20]) Importa recordar que, conforme indicado na secção *4.1 Reparações físicas*, geralmente não se considera que as operações de recondicionamento, manutenção ou reparação constituam modificações substanciais.

([21]) O Regulamento de Execução (UE) 2025/2392 da Comissão estabelece a descrição técnica das categorias de produtos importantes e críticos.

137. A classificação de um produto com elementos digitais como importante ou crítico ou, inversamente, como pertencente à categoria «por defeito» ([22]) é pertinente para determinar o procedimento de avaliação da conformidade que o fabricante tem de seguir, em conformidade com o artigo 32.º, antes de poder colocar esse produto com elementos digitais no mercado. Nomeadamente, os produtos com elementos digitais pertencentes à categoria «por defeito» podem sempre recorrer ao procedimento de controlo interno baseado no módulo A («autoavaliação») ([23]). Os produtos importantes com elementos digitais das classes I ou II e os produtos críticos com elementos digitais estão sujeitos a procedimentos de avaliação da conformidade mais rigorosos. Tal não inclui os produtos importantes com elementos digitais das classes I ou II que se qualifiquem como *software* livre e de código-fonte aberto que estejam colocados no mercado, para os quais, em conformidade com o artigo 32.º, n.º 5, os fabricantes estão autorizados a seguir os procedimentos da categoria «por defeito».

138. Por conseguinte, o conceito de funcionalidade principal é essencial para o fabricante determinar o regime de avaliação da conformidade aplicável. No entanto, este conceito não está explicitamente definido no Regulamento de Ciber-Resiliência. Os produtos com elementos digitais podem desempenhar uma série de funções, algumas das quais podem ser acessórias à funcionalidade principal desse produto, e não devem afetar a classificação do produto como por defeito/importante da classe I/importante da classe II/crítico. Por conseguinte, é útil facultar mais orientações para ajudar os fabricantes a executar corretamente os procedimentos de avaliação da conformidade pertinentes, bem como ajudar as autoridades de fiscalização do mercado a assegurar a aplicação harmonizada do Regulamento de Ciber-Resiliência em toda a UE.

6.1. **Funcionalidade principal**

139. A funcionalidade principal de um produto com elementos digitais refere-se às principais características e capacidades técnicas desse produto, sem as quais este não conseguiria cumprir a sua finalidade prevista. Pode ser avaliada à luz do contexto específico e das condições de utilização desse produto, tendo em conta, nomeadamente, as informações que o fabricante faculta nas instruções de utilização, em materiais e declarações promocionais ou de venda, bem como na documentação técnica.

Exemplo 57: um produto de software *com elementos digitais proporciona um nível de abstração sobre o* hardware *subjacente e gere a execução de componentes do* software*. As suas principais características incluem a inicialização do* hardware *e dos periféricos, a gestão dos processos e da memória, o controlo de entradas/saídas, o agendamento, a afetação de recursos e a exposição dos serviços do sistema e das interfaces de programação de aplicações (IPA) através das quais as aplicações interagem com os recursos de* hardware *e* software *do dispositivo. A documentação técnica indica que o produto com elementos digitais coordena os recursos de computação, aplica configurações do sistema e fornece interfaces normalizadas para módulos de* software *e periféricos conectados. O fabricante destaca estas capacidades como permitindo que a plataforma funcione como o ambiente de* software *central no qual as aplicações podem funcionar de forma fiável. O produto com elementos digitais possui a funcionalidade principal de um sistema operativo, conforme descrito no ponto 11 do anexo I do Regulamento de Execução (UE) 2025/2392.*

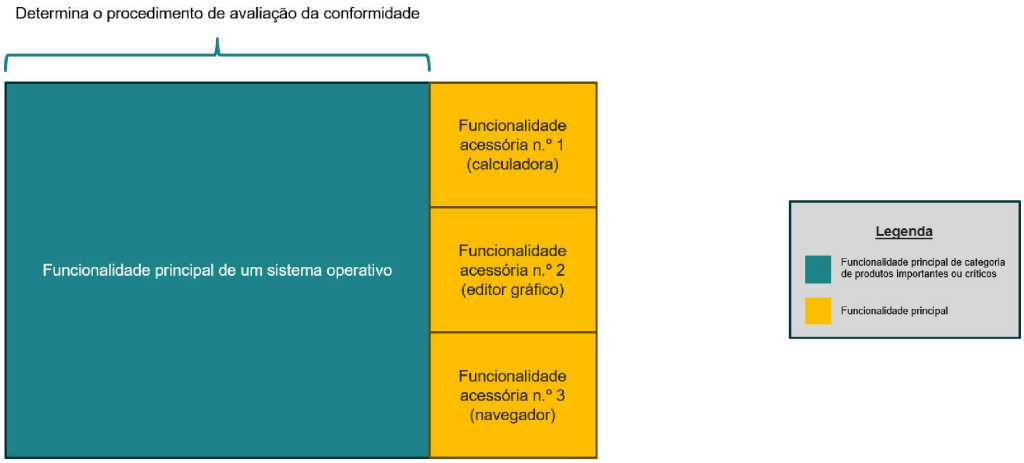
140. É raro a funcionalidade de um produto com elementos digitais se limitar exclusivamente à sua funcionalidade principal, pois os produtos com elementos digitais desempenham frequentemente — se não sempre — funções adicionais que não contribuem para a funcionalidade principal do produto. Tal também pode incluir a incorporação de componentes que possuam, eles próprios, a funcionalidade de outro produto importante ou crítico com elementos digitais. Todavia, o facto de um produto com elementos digitais desempenhar funções diferentes ou adicionais em relação às incluídas nas descrições técnicas de produtos importantes ou críticos com elementos digitais não impede, por si só, que o produto possua uma dessas funcionalidades principais.

([22]) O termo categoria «por defeito» não está definido no Regulamento de Ciber-Resiliência. A utilização do termo no presente documento refere-se a produtos com elementos digitais cuja funcionalidade principal não é a de uma categoria de produtos estabelecida nos anexos III ou IV do Regulamento de Ciber-Resiliência e que, por conseguinte, estão sujeitos ao regime de avaliação da conformidade definido no artigo 32.º, n.º 1.

([23]) Todavia, o fabricante pode sempre optar por aplicar um procedimento de avaliação da conformidade mais rigoroso, conforme previsto no artigo 32.º, n.º 1.

Figura 2:

Ilustração da forma como a funcionalidade principal, e não as funcionalidades acessórias, determinam o procedimento de avaliação da conformidade aplicável



141. Um produto com elementos digitais pode ter a capacidade de desempenhar as funções de uma categoria de produtos importantes ou críticos, mas, ainda assim, possuir uma funcionalidade principal diferente da dessa categoria de produtos. Nesses casos, esse produto com elementos digitais não se qualificaria como um produto importante ou crítico com elementos digitais. Conforme explicitamente referido no artigo 7.º, n.º 1, do Regulamento de Ciber-Resiliência em relação a produtos importantes com elementos digitais (e aplicando a mesma lógica aos produtos críticos com elementos digitais), a mera integração de um produto importante ou crítico com elementos digitais não implica, por si só, que o produto com elementos digitais seja um produto importante ou crítico com elementos digitais.

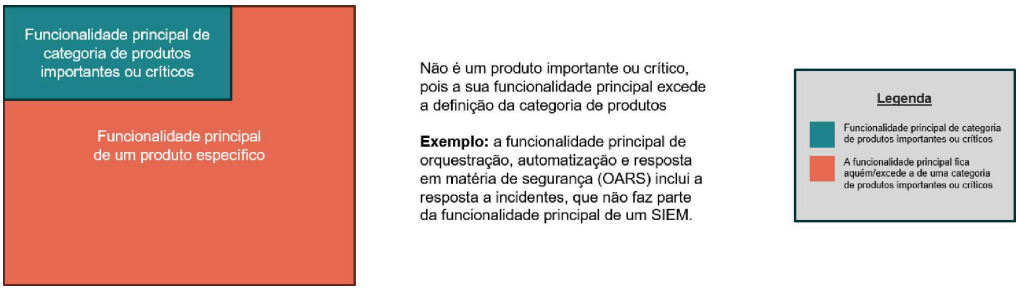
Exemplo 58: um telemóvel inteligente integra um sistema operativo que proporciona as funcionalidades descritas no ponto 11 do anexo I do Regulamento de Execução (UE) 2025/2392. Embora o sistema operativo permita a gestão dos recursos de hardware *e a execução de aplicações informáticas, o telemóvel inteligente no seu todo possui uma funcionalidade principal diferente (por exemplo, permitir que os utilizadores comuniquem e acedam a informações e serviços). A mera integração de um sistema operativo não significa que o telemóvel inteligente possua a funcionalidade principal de um sistema operativo.*

142. Alguns produtos com elementos digitais podem ser semelhantes a uma categoria de produtos importantes ou críticos, ou pertencer à mesma família geral de produtos, mas a sua funcionalidade principal pode exceder substancialmente a funcionalidade principal dessa categoria, ou ficar substancialmente aquém da mesma. Tal não é o caso quando um produto com elementos digitais inclui funcionalidades adicionais que meramente complementam ou melhoram a funcionalidade principal, que, por sua vez, corresponde à de uma categoria de produtos importantes ou críticos. Nesses casos, o produto com elementos digitais mantém a funcionalidade principal dessa categoria e é classificado em conformidade. Esta avaliação deve basear-se nas principais características e nas capacidades técnicas desse produto, tidas objetivamente em conta à luz da sua finalidade prevista, e não na forma como o produto com elementos digitais é descrito ou comercializado, caso essa descrição não reflita as características técnicas reais do produto.

Exemplo 59: um software *de orquestração, automatização e resposta em matéria de segurança (OARS) tem frequentemente a capacidade de desempenhar as funções de produtos com elementos digitais na categoria dos «sistemas de gestão de informações e eventos de segurança (SIEM)», ou seja, recolher dados de várias fontes, analisar e correlacionar esses dados, e apresentá-los como informações práticas para fins de segurança. No entanto, a funcionalidade principal do* software *excede substancialmente a de um sistema SIEM, incluindo serviços como a resposta a incidentes como elementos principais das suas capacidades técnicas. Por conseguinte, geralmente considera-se que o* software *OARS não possui a funcionalidade principal dos sistemas SIEM.*

Figura 3:

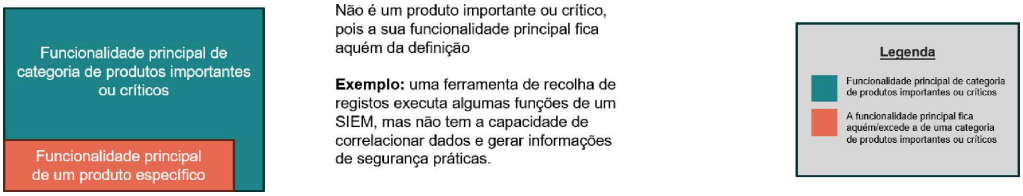
Ilustração da funcionalidade principal de um produto com elementos digitais que excede substancialmente a definição de uma categoria de produtos importantes ou críticos



Exemplo 60: determinadas ferramentas de recolha e visualização de registos possuem a capacidade de incorporar dados de registos e apresentar painéis básicos que mostram eventos do sistema. Embora estas ferramentas possam apoiar as atividades de monitorização da segurança, a sua funcionalidade principal fica aquém da dos sistemas SIEM, pois não realizam a correlação de dados nem facultam informações de segurança práticas. Por conseguinte, geralmente considera-se que essas ferramentas não possuem a funcionalidade principal dos sistemas SIEM.

Figura 4:

Ilustração da funcionalidade principal de um produto com elementos digitais que fica substancialmente aquém da definição de uma categoria de produtos importantes ou críticos

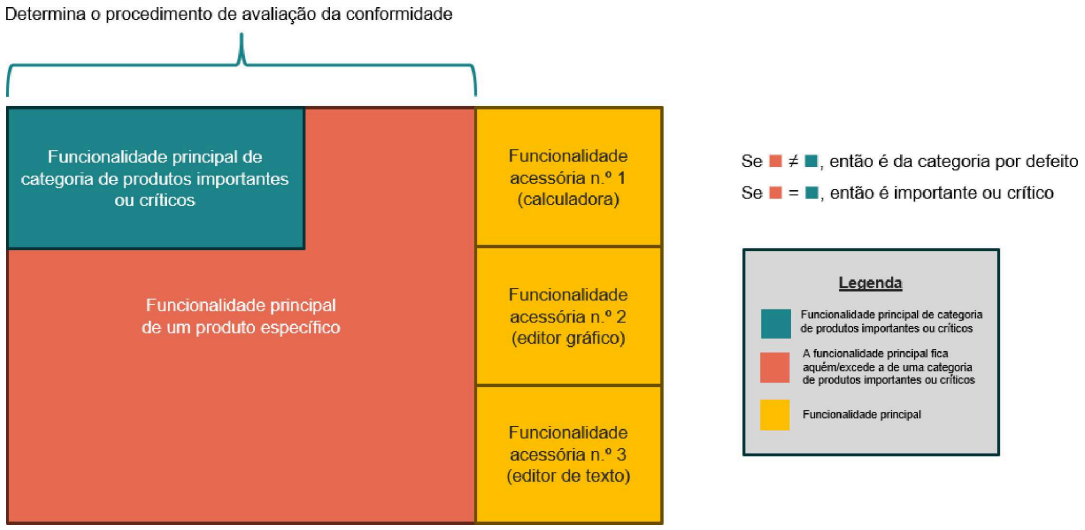


143. Um fabricante não pode deturpar a funcionalidade principal do seu produto com elementos digitais de forma a evadir-se ao regime de avaliação da conformidade aplicável a produtos importantes ou críticos com elementos digitais, por exemplo, salientando ou minimizando excessivamente o papel de determinadas funcionalidades, de modo que o produto exceda substancialmente uma determinada funcionalidade principal, ou fique substancialmente aquém da mesma. Seria o caso, por exemplo, se existissem incoerências evidentes entre os materiais promocionais, as instruções de utilização e a documentação técnica.

144. Um produto com elementos digitais não pode possuir mais do que uma funcionalidade principal para efeitos de determinação do regime de avaliação da conformidade aplicável. De acordo com o anexo VII do Regulamento de Ciber-Resiliência, no âmbito da documentação técnica de um produto, os fabricantes devem descrever a finalidade prevista do seu produto com elementos digitais e o procedimento de avaliação da conformidade que seguiram. Por conseguinte, a funcionalidade principal do produto deve ser claramente identificada. Tal permite a identificação correta do regime de avaliação da conformidade aplicável e que as autoridades de fiscalização do mercado supervisionem e verifiquem se o regulamento está a ser aplicado corretamente.

Figura 5:

Ilustração da forma como a funcionalidade principal de um produto com elementos digitais específico determina a classe de produtos e, por conseguinte, o procedimento de avaliação da conformidade aplicável



145. Alguns produtos com elementos digitais são colocados no mercado como produtos únicos com elementos digitais, mas são compostos por módulos distintos com funcionalidades separadas. Se um fabricante também disponibilizar esses módulos no mercado separadamente, como no caso de serem oferecidos para aquisição, licenciamento ou subscrição separados, esses módulos constituem produtos autónomos com elementos digitais por direito próprio. Como tal, devem ser classificados com base nas respetivas funcionalidades principais (e, por conseguinte, sujeitos ao regime de avaliação da conformidade adequado com base na funcionalidade principal de cada módulo). Tal não prejudica os módulos fornecidos exclusivamente como componentes de um produto integrado com elementos digitais e não disponibilizados separadamente. Nesses casos, a funcionalidade principal é determinada ao nível do produto integrado com elementos digitais.

Exemplo 61: um fabricante coloca no mercado um conjunto de segurança unificado que combina vários módulos, incluindo um SIEM, um sistema de deteção de intrusões e um módulo analítico. O fabricante também disponibiliza esses módulos em subscrições separadas. Neste cenário, cada módulo é um produto com elementos digitais distinto e é classificado com base na sua própria funcionalidade principal. O módulo SIEM está sujeito ao regime de avaliação da conformidade para produtos importantes com elementos digitais da classe I, pois a sua funcionalidade principal é a de «sistemas de gestão de informações e eventos de segurança (SIEM)». O sistema de deteção de intrusões está sujeito ao regime de avaliação da conformidade para produtos importantes com elementos digitais da classe II, pois a sua funcionalidade principal é a de «barreiras de segurança, sistemas de deteção e prevenção de intrusões». O módulo analítico está sujeito ao regime de avaliação da conformidade para produtos com elementos digitais «por defeito», uma vez que a sua funcionalidade principal não é a de uma categoria de produtos importantes ou críticos.

146. O incumprimento das obrigações estabelecidas no artigo 32.º do Regulamento de Ciber-Resiliência pode dar origem a coimas nos termos do artigo 64.º, n.º 3.

6.2. Avaliação da conformidade para produtos importantes e críticos com elementos digitais

147. Depois de determinar a funcionalidade principal do seu produto com elementos digitais, o fabricante tem de realizar um dos procedimentos de avaliação da conformidade aplicáveis. O fabricante deve assegurar que o produto com elementos digitais no seu todo cumpre os requisitos essenciais, tendo em conta, se for caso disso, a segurança dos componentes ou funcionalidades nele integrados.

148. É obrigatório um procedimento de avaliação da conformidade mais rigoroso, com a participação de um terceiro (com base nos módulos B+C, no módulo H ou em sistemas de certificação da cibersegurança), para os produtos importantes com elementos digitais da classe II (com exceção dos que se qualificam como *software* livre e de código-fonte aberto, em conformidade com o artigo 32.º, n.º 5) e para os produtos críticos com elementos digitais ([24]). Em contrapartida, os produtos importantes com elementos digitais da classe I (com exceção dos que se qualificam como *software* livre e de código-fonte aberto, em conformidade com o artigo 32.º, n.º 5) só são obrigados a ser submetidos a um procedimento de avaliação da conformidade por terceiros se o fabricante não tiver aplicado, ou tiver aplicado apenas parcialmente, as normas harmonizadas pertinentes cujas referências tenham sido publicadas no *Jornal Oficial da União Europeia* (a seguir designadas por «normas harmonizadas»), as especificações comuns ou os sistemas europeus de certificação da cibersegurança com um nível de garantia que seja, pelo menos, «substancial» ([25]).

149. Por conseguinte, para que um produto importante com elementos digitais da classe I seja elegível para o procedimento de controlo interno, i) todos os requisitos aplicáveis de uma norma harmonizada pertinente têm de ser aplicados e ii) o âmbito da norma tem de abranger, pelo menos, todos os riscos de cibersegurança associados à funcionalidade principal desse produto.

150. O âmbito do produto com elementos digitais pode ser mais vasto do que o previsto pela norma harmonizada pertinente e essas funções adicionais podem apresentar riscos de cibersegurança diferentes ou adicionais. O fabricante é sempre obrigado a realizar uma avaliação dos riscos, por força do artigo 13.º, n.º 2, devendo, por conseguinte, verificar se a aplicação de uma norma harmonizada abrange todos os riscos associados ao produto com elementos digitais. Caso a aplicação da norma não abranja todos os riscos, o fabricante deverá assegurar, por outros meios, que o seu produto com elementos digitais está em conformidade com os requisitos essenciais.

151. Por conseguinte, se o fabricante de um produto importante com elementos digitais da classe I tiver aplicado uma norma harmonizada pertinente que abranja os riscos associados à funcionalidade principal desse produto, pode decidir recorrer ao procedimento de controlo interno para demonstrar a conformidade do seu produto. No âmbito das suas atividades de avaliação da conformidade, o fabricante continuará a ser obrigado a demonstrar que todos os riscos aplicáveis ao seu produto com elementos digitais são tidos em conta. Por conseguinte, caso exista uma lacuna entre a cobertura da norma harmonizada e o âmbito do produto com elementos digitais no seu todo, o fabricante continua a ter de documentar as medidas adicionais que adotou para tratar esses riscos.

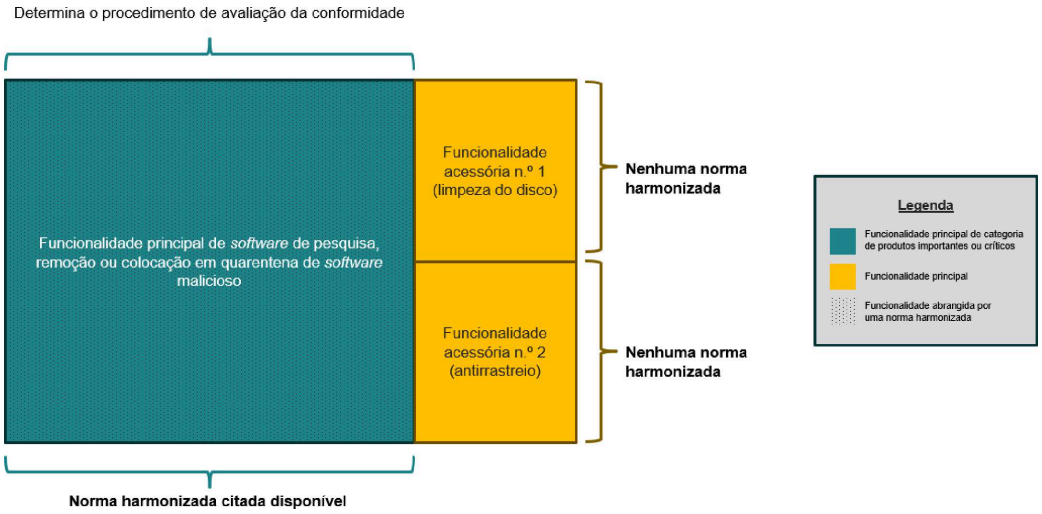
Exemplo 62: um software *antivírus possui a funcionalidade principal de* software *de pesquisa, remoção ou colocação em quarentena de* software *malicioso, conforme descrito no ponto 4 do anexo I do Regulamento de Execução (UE) 2025/2392. Esse produto com elementos digitais também inclui funcionalidades adicionais, nomeadamente uma função de limpeza do disco e uma função antirrastreio que protege o utilizador ao navegar na Web. O fabricante realiza uma avaliação dos riscos que abrange o produto com elementos digitais na sua totalidade, incluindo a funcionalidade principal do antivírus, a limpeza do disco e as funções antirrastreio. Aplica uma norma harmonizada que abrange os riscos associados à funcionalidade principal do antivírus e medidas adicionais para fazer face aos riscos decorrentes de funções adicionais. O fabricante está autorizado a utilizar o procedimento de controlo interno para a sua avaliação da conformidade, abrangendo o produto com elementos digitais no seu todo, incluindo as funções de limpeza do disco e de antirrastreio.*

([24]) É também o caso quando se recorre a um sistema europeu de certificação da cibersegurança com um nível de garantia que seja, pelo menos, «substancial», pois é necessária a participação de um organismo de certificação por terceiros.

([25]) Por uma questão de brevidade, a parte restante da presente secção refere-se apenas às normas harmonizadas cujas referências tenham sido publicadas no *Jornal Oficial da União Europeia*. Todavia, as mesmas orientações também se aplicam às especificações comuns adotadas em conformidade com o artigo 27.º, n.º 2, e aos sistemas europeus de certificação da cibersegurança especificados pela Comissão por meio de atos delegados em conformidade com o artigo 27.º, n.º 9.

Figura 6:

Ilustração da forma como a utilização de uma norma harmonizada citada que abranja apenas a funcionalidade principal determina o procedimento de avaliação da conformidade aplicável



152. É também o caso quando o produto com elementos digitais integra uma função adicional que é, ela própria, a de outro produto importante ou crítico com elementos digitais. Com efeito, é a funcionalidade principal do produto com elementos digitais no seu todo, e não a funcionalidade dos componentes integrados considerados isoladamente, que determina se o produto com elementos digitais pertence à categoria de produtos importantes ou críticos (e, por conseguinte, o regime de avaliação da conformidade aplicável). Por exemplo, se um produto com elementos digitais possuir a funcionalidade principal de um produto importante com elementos digitais da classe I, esse produto no seu todo está sujeito ao regime de avaliação da conformidade aplicável aos produtos importantes com elementos digitais da classe I, apesar de integrar um componente que é, ele próprio, um produto crítico com elementos digitais. Nestes casos, se o fabricante aplicar uma norma harmonizada que abranja os riscos associados à funcionalidade principal desse produto, pode recorrer ao procedimento de controlo interno.

Exemplo 63: um produto de hardware *com elementos digitais possui a funcionalidade principal de um encaminhador, conforme descrito no ponto 12 do anexo I do Regulamento de Execução (UE) 2025/2392. Esse produto com elementos digitais também inclui funcionalidades adicionais, nomeadamente capacidades de barreira de segurança* (firewall)*, pois integra um componente de barreira de segurança. O fabricante realiza uma avaliação dos riscos que abrange o produto com elementos digitais na sua totalidade, incluindo a funcionalidade principal do encaminhador e a funcionalidade de barreira de segurança. Aplica uma norma harmonizada que abrange os riscos associados à funcionalidade principal do encaminhador e medidas adicionais para fazer face aos riscos decorrentes de funções adicionais. Por exemplo, o fabricante pode aplicar a norma harmonizada relativa às barreiras de segurança, a fim de abranger os riscos associados à funcionalidade de barreira de segurança. O fabricante está autorizado a utilizar o procedimento de controlo interno para a sua avaliação da conformidade, abrangendo o produto com elementos digitais no seu todo, incluindo a funcionalidade de barreira de segurança.*

6.3. Implicações para a presunção de conformidade

153. O artigo 27.º, n.º 1, do Regulamento de Ciber-Resiliência estabelece que se presume 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* (JOUE), estão conformes com os requisitos essenciais constantes do Regulamento de Ciber-Resiliência, abrangidos pelas referidas normas ou

partes destas ([26]). O artigo 27.º, n.º 5, alarga a mesma presunção de conformidade aos produtos com elementos digitais e aos processos aplicados pelo fabricante que estejam em conformidade com as especificações comuns estabelecidas pela Comissão por meio de atos de execução, e o artigo 27.º, n.º 8, estabelece a presunção de conformidade dos produtos com elementos digitais e dos 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, se tal tiver sido especificado por meio de atos delegados nos termos do artigo 27.º, n.º 9 ([27]).

154. Por conseguinte, se o fabricante tiver aplicado uma norma harmonizada cujas referências tenham sido publicadas no JOUE, beneficia de uma presunção de conformidade em relação aos riscos abrangidos por essa norma. Tal pode ser o caso, por exemplo, quando a norma harmonizada referenciada aborda todos os riscos associados à funcionalidade principal de um produto com elementos digitais e não existem funcionalidades adicionais que apresentem riscos de cibersegurança. Por exemplo, espera-se que a norma harmonizada para encaminhadores dê resposta, pelo menos, aos riscos associados à funcionalidade principal destes produtos com elementos digitais. Se esse produto não contiver quaisquer funcionalidades adicionais ou se essas funcionalidades adicionais não apresentarem riscos que não são abordados pela norma, o produto com elementos digitais pode beneficiar da presunção de conformidade.

155. Nos casos referidos nos pontos 151 e 152, o fabricante está autorizado a utilizar o procedimento de controlo interno, uma vez que a norma harmonizada abrange os riscos associados à funcionalidade principal do produto com elementos digitais. Todavia, os produtos com elementos digitais descritos nesses exemplos podem ser mais vastos do que o âmbito de aplicação das normas harmonizadas e as funcionalidades adicionais podem apresentar riscos de cibersegurança que não são abordados por essa norma harmonizada. Por conseguinte, esses produtos com elementos digitais não podem beneficiar da presunção de conformidade em relação a essas funcionalidades adicionais.

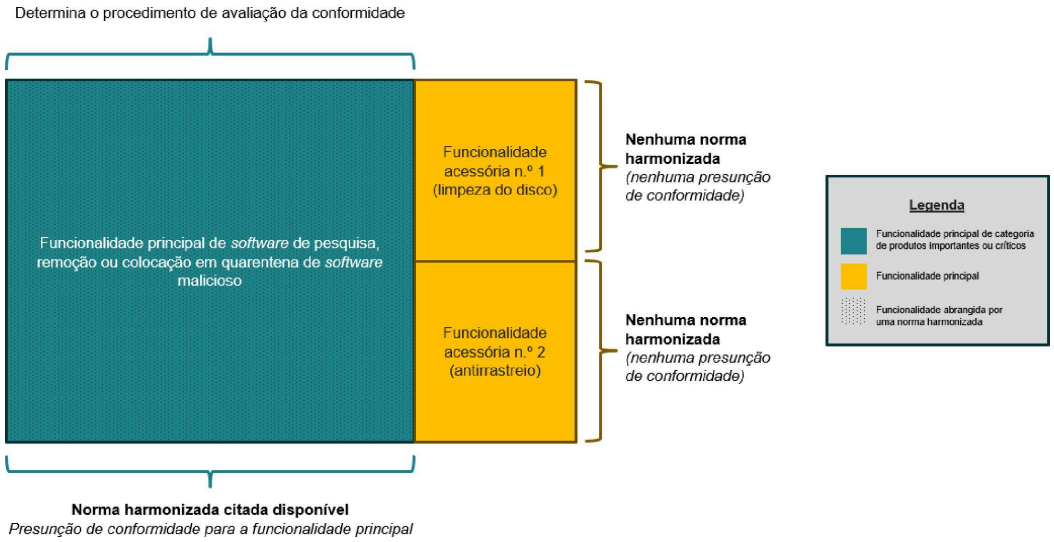
Exemplo 64: um software *antivírus possui a funcionalidade principal de* software *de pesquisa, remoção ou colocação em quarentena de* software *malicioso, e a norma harmonizada abrange os riscos associados a essa funcionalidade principal. Esse produto com elementos digitais também inclui funcionalidades adicionais, nomeadamente uma função de limpeza do disco e uma funcionalidade antirrastreio que protege o utilizador ao navegar na Web, cujos riscos a norma harmonizada não abrange. Se a norma harmonizada for aplicada, o fabricante está autorizado a recorrer ao procedimento de controlo interno para a sua avaliação da conformidade. Beneficiará da presunção de conformidade em relação aos riscos associados à funcionalidade principal desse produto, mas não em relação aos riscos associados às funcionalidades adicionais.*

([26]) Conforme claramente indicado na secção 4.1.2.2 do Guia Azul, «[n]a legislação de harmonização relativa aos riscos [...] os fabricantes, mesmo quando utilizam normas harmonizadas cujas referências estão publicadas no *Jornal Oficial da União Europeia*, continuam a ser plenamente responsáveis pela avaliação de todos os riscos dos seus produtos a fim de determinar quais os requisitos essenciais (ou outros) aplicáveis. Após essa avaliação, o fabricante pode optar por aplicar as especificações técnicas contidas em normas harmonizadas cujas referências estão publicadas no *Jornal Oficial da União Europeia*, a fim de aplicar "medidas de redução dos riscos" especificadas nas normas harmonizadas».

([27]) Tal como anteriormente, por uma questão de brevidade, a parte restante da presente secção refere-se apenas às normas harmonizadas cujas referências tenham sido publicadas no *Jornal Oficial da União Europeia*. Contudo, as mesmas orientações também se aplicam às especificações comuns e aos sistemas europeus de certificação da cibersegurança.

Figura 7:

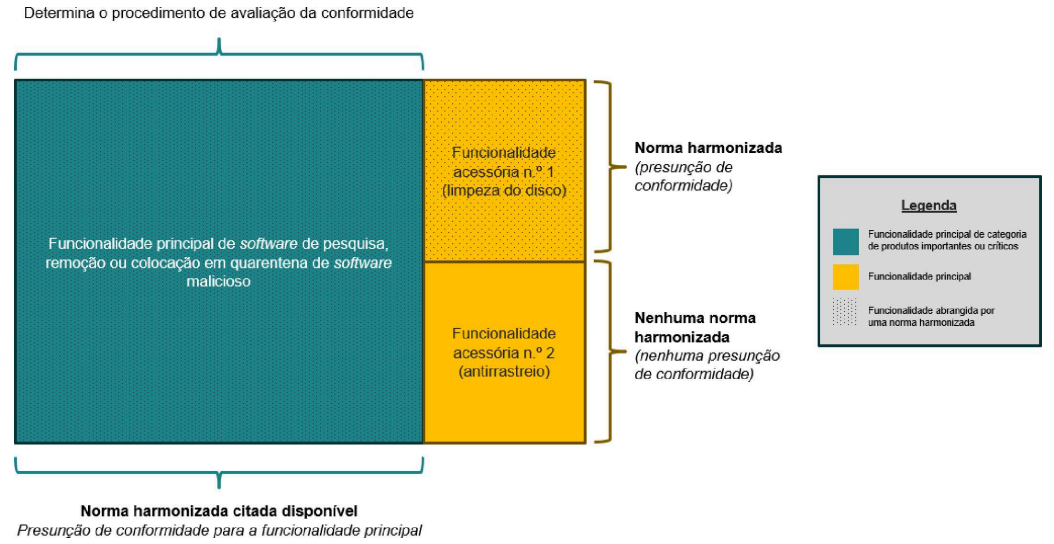
A norma harmonizada concede a presunção de conformidade em relação à funcionalidade principal, uma vez que aborda todos os riscos associados a essa funcionalidade principal, mas não em relação às funcionalidades acessórias



Exemplo 65: no mesmo cenário que o exemplo anterior, a norma harmonizada foi agora atualizada de modo a abranger também os riscos associados a uma das funcionalidades adicionais, a saber, a função de limpeza do disco, mas não a outra (ou seja, a função antirrastreio). Se a norma harmonizada for aplicada, o fabricante está autorizado a recorrer ao procedimento de controlo interno para a sua avaliação da conformidade. Beneficiará de uma presunção de conformidade em relação aos riscos associados à funcionalidade principal desse produto e à funcionalidade de limpeza do disco, mas não em relação aos riscos relacionados com a funcionalidade antirrastreio.

Figura 8:

A norma harmonizada concede a presunção de conformidade em relação à funcionalidade principal e à funcionalidade acessória n.º 1, uma vez que aborda todos os riscos associados a essas duas funcionalidades, mas não em relação à funcionalidade acessória n.º 2



7. AVALIAÇÃO DOS RISCOS DE CIBERSEGURANÇA E INTEGRAÇÃO DE PRODUTOS COM ELEMENTOS DIGITAIS E COMPONENTES

7.1. Sobre a avaliação e o tratamento dos riscos de cibersegurança

156. A avaliação dos riscos de cibersegurança prevista no artigo 13.º, n.º 2, do Regulamento de Ciber-Resiliência exige que os fabricantes identifiquem os riscos pertinentes e avaliem o seu potencial impacto no produto com elementos digitais. Os fabricantes devem igualmente aplicar medidas adequadas para fazer face a esses riscos, em conformidade com os requisitos essenciais constantes do anexo I.

157. Na gestão do risco organizativo, os riscos são geralmente avaliados em função de critérios de aceitação derivados dos objetivos internos ou da apetência pelo risco da organização. Em contrapartida, nos termos do Regulamento de Ciber-Resiliência, deve avaliar-se o risco de cibersegurança residual à luz do requisito de que o produto com elementos digitais colocado no mercado garanta um nível adequado de cibersegurança com base nos riscos, tendo em conta a sua finalidade prevista e a sua utilização razoavelmente previsível.

158. Por conseguinte, a tolerância interna ao risco, a estratégia comercial ou meras considerações de custos do fabricante não são pertinentes para determinar se os riscos foram abordados. Para efeitos do artigo 13.º, n.ºs 2 e 3, os fabricantes devem estar em condições de determinar se os riscos de cibersegurança identificados foram suficientemente abordados através da aplicação dos requisitos essenciais constantes da parte I do anexo I, à luz da finalidade prevista, da utilização razoavelmente previsível e das condições de utilização, incluindo, se for caso disso, o ambiente operacional (por exemplo, os utilizadores previstos do produto com elementos digitais) e os ativos a proteger, tendo em conta o período de utilização previsível do produto com elementos digitais.

159. O risco de cibersegurança residual é um resultado inerente da avaliação e do tratamento dos riscos. Reconhece-se que, na prática, não é possível eliminar totalmente os riscos de cibersegurança. Todavia, a existência de um risco residual não implica que qualquer risco possa ser aceite ao critério do fabricante. Um produto com elementos digitais só pode ser colocado no mercado se os riscos residuais, após se tomarem as medidas adequadas, tiverem sido suficientemente abordados através da aplicação dos requisitos essenciais, tendo em conta a finalidade prevista e a utilização razoavelmente previsível do produto com elementos digitais.

160. Em conformidade com o artigo 13.º, n.º 3, caso sejam identificados riscos de cibersegurança, os fabricantes são obrigados a dar-lhes resposta através de medidas adequadas, nomeadamente a nível dos produtos. Dependendo das circunstâncias, tal pode envolver, por exemplo, a redução da superfície de ataque, a aplicação de salvaguardas técnicas, a limitação ou adaptação da funcionalidade, ou a definição mais precisa da finalidade prevista do produto com elementos digitais. Os fabricantes também podem tomar medidas para moldar a utilização razoavelmente previsível do produto com elementos digitais, por exemplo através da comunicação dos riscos, de orientações aos utilizadores ou da conceção da interface de utilizador, a fim de orientar o comportamento dos utilizadores para padrões de utilização seguros.

161. O Regulamento de Ciber-Resiliência não prevê a transferência de riscos de cibersegurança ou responsabilidade para os utilizadores ou terceiros a fim de compensar deficiências na conceção dos produtos ou justificar a falta de resposta a esses riscos. A obrigação de colocar no mercado um produto com elementos digitais seguro e de demonstrar a conformidade com os requisitos essenciais continua a caber ao fabricante.

162. As informações e instruções facultadas aos utilizadores podem ser utilizadas para apoiar a implantação e o funcionamento seguros do produto com elementos digitais, incluindo caso o fabricante tenha optado por restringir a finalidade prevista desse produto a ambientes de confiança, e para informar os utilizadores dos riscos residuais, de uma forma adequada à natureza do produto com elementos digitais e aos utilizadores a que se destina.

Exemplo 66: um fabricante desenvolve um sensor industrial para utilização em ambientes de confiança. Para que o sensor desempenhe a sua funcionalidade corretamente, o fabricante não aplica medidas de proteção contra ataques físicos ao próprio sensor. A fim de atenuar os riscos associados identificados na avaliação dos riscos, o fabricante limita a finalidade prevista do sensor à utilização apenas em ambientes de confiança em que seja impedido o acesso físico não autorizado ao produto com elementos digitais. As informações e instruções destinadas aos utilizadores proporcionam informações claras sobre estas limitações à utilização do sensor, de uma forma adequada à natureza do produto com elementos digitais e aos utilizadores a que se destinam.

Exemplo 67: um fabricante desenvolve uma aplicação informática para utilização profissional em computadores de secretária e dispositivos móveis geridos. A aplicação procede ao tratamento de dados sensíveis armazenados localmente e conteúdos gerados pelos utilizadores. Durante a avaliação dos riscos, o fabricante identifica o risco de acesso não autorizado a esses dados, se forem armazenados em texto transparente no dispositivo. Em vez de conceber e implementar um mecanismo de cifragem proprietário na própria aplicação, o fabricante opta por recorrer às funções de cifragem e de gestão de chaves disponibilizadas nativamente pelo sistema operativo no qual a aplicação se destina a funcionar, uma vez que os serviços criptográficos integrados do sistema operativo estão maduros e são objeto de manutenção periódica.

163. Caso a avaliação dos riscos de cibersegurança identifique riscos que não possam ser devidamente abordados através de medidas adequadas, a conformidade com o Regulamento de Ciber-Resiliência pode exigir alterações da conceção, da funcionalidade ou da finalidade prevista do produto com elementos digitais. Considerações relacionadas exclusivamente com os custos ou a viabilidade comercial não constituem motivos suficientes para deixar esses riscos por tratar, se tal impedir o produto com elementos digitais de cumprir os requisitos essenciais.

7.2. Sobre a conceção, desenvolvimento e produção de produtos com elementos digitais de modo a garantir um nível adequado de cibersegurança com base nos riscos

164. O requisito essencial de cibersegurança a que se refere a parte I, ponto 1, do anexo I do Regulamento de Ciber-Resiliência prevê que os produtos com elementos digitais sejam concebidos, desenvolvidos e produzidos de modo a garantir um nível adequado de cibersegurança com base nos riscos.

165. Este requisito essencial visa dar resposta a todos os riscos de cibersegurança identificados no âmbito da avaliação dos riscos de cibersegurança, incluindo, em especial, os riscos de cibersegurança que não são adequadamente abordados, de qualquer outra forma, no âmbito da aplicação dos requisitos essenciais constantes de outros pontos da parte I do anexo I que não sejam o ponto 1. Este requisito essencial é diferente da obrigação legal de realizar uma avaliação dos riscos de cibersegurança, que deve ser realizada nos termos do artigo 13.º, n.º 2.

166. Caso todos os riscos de cibersegurança pertinentes relacionados com um produto com elementos digitais sejam tratados através da aplicação de medidas adequadas para dar resposta aos requisitos essenciais aplicáveis constantes de outros pontos que não o ponto 1, considera-se cumprido o requisito essencial a que se refere a parte I, ponto 1, do anexo I. Em contrapartida, caso a avaliação dos riscos de cibersegurança identifique riscos adicionais que essas medidas não abordam plenamente, os fabricantes são obrigados a aplicar medidas adequadas ao produto com elementos digitais para fazer face a esses riscos, a fim de cumprirem o requisito essencial a que se refere a parte I, ponto 1, do anexo I. Na prática, na maioria dos casos, espera-se que a conformidade com os outros requisitos essenciais resulte na conformidade com este requisito.

7.3. Avaliação dos riscos e diligência devida em relação às dependências externas e aos componentes integrados

167. O Regulamento de Ciber-Resiliência estabelece duas obrigações distintas, mas complementares, para os fabricantes no que diz respeito à gestão dos riscos de cibersegurança. Em primeiro lugar, o artigo 13.º, n.º 2, exige que os fabricantes efetuem uma avaliação dos riscos de cibersegurança para o próprio produto com elementos digitais. Em segundo lugar, o artigo 13.º, n.º 5, impõe a obrigação de exercer a diligência devida no que diz respeito aos componentes integrados. Em conjunto, estas duas obrigações destinam-se a assegurar que o produto com elementos digitais continua a ser seguro, nomeadamente quando recorre a soluções de tratamento remoto de dados, serviços remotos, ou componentes de *software* ou *hardware* de terceiros.

168. A avaliação dos riscos de cibersegurança diz respeito à identificação e gestão de riscos pertinentes que possam afetar o produto com elementos digitais, incluindo riscos que tenham origem fora do próprio produto, como redes externas, fatores ambientais ou outros aspetos externos que possam afetar o produto com elementos digitais ou aos quais o produto recorra. Para esses riscos externos, o Regulamento de Ciber-Resiliência não exige que os fabricantes controlem ou regulem o ambiente externo. Em vez disso, os fabricantes são obrigados a identificar esses riscos e a atenuá-los através da conceção e do desenvolvimento do próprio produto com elementos digitais, o que implicará a aplicação dos requisitos essenciais adequados estabelecidos na parte I do anexo I e, se necessário, a prestação de informações e instruções aos utilizadores sobre os riscos de integração ou implantação.

169. Por exemplo, um fabricante pode identificar um risco de pessoas não autorizadas poderem obter acesso a sistemas de retaguarda que não fazem parte do próprio produto com elementos digitais enquanto o produto está em funcionamento e tentarem enviar comandos maliciosos ao produto com elementos digitais. Esses sistemas de retaguarda, caso não sejam concebidos e desenvolvidos pelo fabricante ou sob a sua responsabilidade, ou caso não suportem uma das funções do produto com elementos digitais, não constituem soluções de tratamento remoto de dados e, por conseguinte, não são abrangidos pelo âmbito do produto com elementos digitais para efeitos do Regulamento de Ciber-Resiliência. No entanto, o Regulamento de Ciber-Resiliência exige que o fabricante dê resposta ao risco que podem representar através de medidas a nível do produto, nomeadamente ao exigir a autenticação criptográfica de comandos remotos, verificar a integridade das alterações da configuração ou gerar registos ou alertas pertinentes para a segurança quando é detetado um comportamento anormal. Do mesmo modo, caso um serviço externo fique indisponível, por exemplo devido a cortes de energia ou a falhas da infraestrutura, e um fabricante identificar um risco resultante dessa indisponibilidade, o Regulamento de Ciber-Resiliência pode exigir medidas de atenuação a nível do produto contra esses riscos de cibersegurança — por exemplo, assegurar que a indisponibilidade não faz com que o produto com elementos digitais entre em estados inseguros. Nesses casos, o Regulamento de Ciber-Resiliência regula a forma como o produto com elementos digitais dá resposta a esses riscos externos. Não impõe obrigações sobre o modo como a infraestrutura de retaguarda é organizada, dotada de pessoal ou explorada, nem trata essa infraestrutura como sendo parte do produto com elementos digitais.

170. A diligência devida diz respeito aos elementos que fazem parte do próprio produto com elementos digitais, em especial componentes integrados de *software* ou *hardware* fornecidos por terceiros. Os fabricantes são obrigados a tomar medidas adequadas para assegurar que esses componentes não comprometem a conformidade do produto com elementos digitais com os requisitos essenciais. Tal só pode ser alcançado ao determinar o que o produto com elementos digitais exige dos seus componentes para cumprir os seus objetivos de cibersegurança e ao verificar, de uma forma baseada no risco, se esses componentes estão em consonância com as necessidades do produto, conforme indicado também no considerando 34.

171. Em consonância com a sua avaliação dos riscos de cibersegurança, o fabricante tem de identificar os requisitos que o componente integrado deve cumprir. Por exemplo, se o produto com elementos digitais recorrer a funções criptográficas, mecanismos de atualização ou comunicações seguras fornecidas por um componente, o fabricante deve, no âmbito da sua diligência devida, identificar essas necessidades e verificar se o componente as cumpre. As provas para este efeito podem consistir em documentação obtida junto do fabricante do componente, como especificações técnicas, documentação de segurança ou documentação de conformidade ou de garantia pertinente. Se for caso disso, o fabricante também pode realizar ensaios para verificar se esses componentes desempenham adequadamente as funções pertinentes. Embora a diligência devida seja uma obrigação jurídica distinta, apoia e sustenta a capacidade do fabricante para demonstrar a conformidade com os requisitos essenciais aplicáveis ao produto com elementos digitais no seu todo.

172. Ao avaliar os riscos para o produto com elementos digitais no seu todo, os elementos exteriores ao produto, como elementos ambientais, infraestruturas externas, outros sistemas ou redes, devem ser tidos em conta na avaliação dos riscos de cibersegurança e, se for caso disso, abordados através de medidas a nível do produto para assegurar a conformidade do produto com elementos digitais com os requisitos essenciais. Os componentes que estão física ou logicamente integrados no produto com elementos digitais, mas que são provenientes de terceiros, também devem ser considerados como parte da avaliação dos riscos. Todavia, para efeitos de conformidade, o fabricante deve tratá-los como componentes fornecidos externamente, cujas propriedades são verificadas através da diligência devida após a integração, uma vez que o fabricante pode não os ter reformulado ou reconvertido.

173. Aplica-se a mesma lógica durante o desenvolvimento e a integração de componentes. Caso o fabricante desenvolva funcionalidades ele próprio, deve aplicar diretamente os requisitos essenciais. Se o fabricante integrar componentes desenvolvidos por terceiros, deve assegurar, através da diligência devida, que esses componentes podem ser utilizados de uma forma que o produto com elementos digitais no seu todo possa cumprir. Em ambos os casos, o objetivo continua a ser o mesmo: que o produto com elementos digitais, tal como colocado no mercado, atinja um nível adequado de cibersegurança, conforme exigido pelo Regulamento de Ciber-Resiliência, tendo em conta os riscos identificados na avaliação dos riscos de cibersegurança.

7.4. **Reutilização de avaliações dos riscos e de documentação de conformidade para famílias de produtos com elementos digitais**

174. Os fabricantes podem colocar no mercado produtos com elementos digitais semelhantes, por exemplo diferentes variantes, modelos ou configurações da mesma família de produtos. Caso esses produtos com elementos digitais partilhem a mesma arquitetura, conceção pertinente para a segurança e finalidade prevista, e estejam expostos aos mesmos riscos de cibersegurança, o Regulamento de Ciber-Resiliência não exige que os fabricantes tratem cada variante como um produto com elementos digitais totalmente separado para efeitos de avaliação dos riscos e de avaliação da conformidade.

175. Nesses casos, desde que todas as variantes em causa estejam devidamente abrangidas em termos de riscos pertinentes e requisitos essenciais, os fabricantes podem recorrer: i) a uma avaliação única dos riscos de cibersegurança realizada em conformidade com o artigo 13.º, n.º 2, do Regulamento de Ciber-Resiliência, ii) a um conjunto único de documentação técnica e iii) a um procedimento único de avaliação da conformidade. Tal permite igualmente a emissão de uma única declaração de conformidade UE para o grupo de produtos com elementos digitais, desde que identifique claramente as variantes do produto às quais se aplica.

176. O fator decisivo consiste em saber se as diferenças entre as variantes são pertinentes para a cibersegurança. As variações que não afetem as propriedades de cibersegurança do produto com elementos digitais, como diferenças de cor, fator de forma, dimensão da memória ou outras características que não são pertinentes para a segurança, não exigem avaliações dos riscos ou avaliações da conformidade separadas. Em contrapartida, em alguns casos, as variantes podem diferir de formas que afetem a aplicação dos requisitos essenciais, por exemplo, através de diferentes interfaces de comunicação, pilhas de *software*, mecanismos de atualização ou conectividade à distância. Nesses casos, essas diferenças devem refletir-se na avaliação dos riscos e, se necessário, na avaliação da conformidade e na documentação técnica.

177. Os fabricantes continuam a ser responsáveis por assegurar que a avaliação dos riscos e a documentação conexa refletem com exatidão os produtos com elementos digitais colocados no mercado. Caso uma nova variante introduza novos riscos de cibersegurança ou altere a forma como os requisitos essenciais são aplicados, a avaliação dos riscos e a documentação de conformidade existentes devem ser atualizadas em concordância. O recurso a uma única avaliação da conformidade só é possível na medida em que os produtos com elementos digitais não apresentem diferenças no que diz respeito às suas propriedades de cibersegurança.

8. **TRATAMENTO REMOTO DE DADOS**

178. O artigo 3.º, ponto 1, do Regulamento de Ciber-Resiliência define «produto com elementos digitais» como «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». Neste contexto, o fabricante deve ter em conta o produto com elementos digitais no seu todo, incluindo as suas soluções de tratamento remoto de dados. Por exemplo, ao demonstrar que o produto com elementos digitais cumpre os requisitos essenciais estabelecidos no anexo I, as soluções de tratamento remoto de dados devem ser tidas em conta, a começar pela avaliação dos riscos (artigo 13.º, n.º 2). O mesmo se aplica às obrigações decorrentes do ciclo de vida, como a comunicação de vulnerabilidades ativamente exploradas e de incidentes graves (artigo 14.º).

179. O objetivo das presentes orientações consiste em prestar mais apoio aos fabricantes ao determinarem se o seu produto com elementos digitais possui soluções de tratamento remoto de dados, conforme definido no Regulamento de Ciber-Resiliência, e como cumprir as suas obrigações de conformidade a este respeito. Após uma análise inicial das definições e dos considerandos constantes do Regulamento de Ciber-Resiliência, as presentes orientações apresentarão perguntas para ajudar os fabricantes a esclarecer se o seu produto com elementos digitais inclui soluções de tratamento remoto de dados (ver a secção *8.1 O que se considera ser uma solução de tratamento remoto de dados para um* produto com elementos digitais?). Posteriormente, aprofundará as implicações técnicas das soluções de tratamento remoto de dados e como avaliar a conformidade com o Regulamento de Ciber-Resiliência (ver a secção *8.2 Implicações práticas e técnicas das soluções de tratamento remoto de dados e recurso a* soluções de terceiros).

180. Com efeito, no artigo 3.º, ponto 2, define-se «tratamento remoto de dados» como «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». Por conseguinte, as soluções de tratamento remoto de dados são definidas como os elementos de *software* («a parte de um sistema de informação eletrónico que consiste em código de computador», conforme definição constante do artigo 3.º, ponto 4) do tratamento de dados à distância. Não se destina a incluir, como parte do âmbito do produto com elementos digitais, o *hardware* ao qual o tratamento remoto de dados pode recorrer.

181. Os considerandos 11 e 12 facultam explicações adicionais sobre como este conceito deve ser interpretado. O considerando 11 esclarece que o objetivo de abranger a solução de tratamento remoto de dados é garantir «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». Também estabelece que «[o]s 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».

182. Por conseguinte, resulta do considerando 11 que a intenção não consiste em fazer com que os requisitos constantes do Regulamento de Ciber-Resiliência abranjam toda a infraestrutura informática de uma organização, mas apenas os componentes de *software* que permitem a execução da solução de tratamento de dados. Por exemplo, os sistemas internos relacionados com os recursos humanos próprios do fabricante, as folhas de pagamentos, a gestão das relações com os clientes, os *pipelines* de integração contínua/entrega contínua (CI/CD) e a distribuição de atualizações de segurança a localizações periféricas não devem ser considerados soluções de tratamento remoto de dados. Do mesmo modo, os sistemas associados a atividades de auditoria e ensaio, como os testes de penetração, a deteção proativa de ameaças e a simulação de ataques, estão fora do âmbito de um produto com elementos digitais conforme abrangido pelo Regulamento de Ciber-Resiliência. Importa notar que, embora a aplicação de ensaios e análises eficazes e regulares da segurança do produto com elementos digitais seja um requisito essencial estabelecido na parte II, ponto 3, do anexo I do Regulamento de Ciber-Resiliência, tal não significa que essas atividades devam ser consideradas soluções de tratamento remoto de dados para o produto com elementos digitais.

183. O considerando 12 centra-se nos serviços de computação em nuvem e desenvolve as circunstâncias em que esses serviços podem ser considerados soluções de tratamento remoto de dados. O considerando conclui recordando que os serviços de computação em nuvem e os modelos de serviços de computação em nuvem são abrangidos pelo âmbito de aplicação da Diretiva (UE) 2022/2555 (Diretiva SRI 2) ([28]), que estabelece requisitos de gestão dos riscos de cibersegurança para os prestadores de serviços de computação em nuvem. Esses requisitos são especificados mais pormenorizadamente no Regulamento de Execução (UE) 2024/2690 da Comissão ([29]).

8.1. **O que se considera ser uma solução de tratamento remoto de dados para um produto com elementos digitais?**

184. A definição de «tratamento remoto de dados» estabelecida no artigo 3.º, ponto 2, assenta em três elementos: i) se o tratamento de dados é efetuado «à distância», ii) se a inexistência desse tratamento de dados impediria o produto com elementos digitais de desempenhar uma das suas funções e iii) se o *software* foi concebido e desenvolvido pelo fabricante ou sob a sua responsabilidade. As três subsecções seguintes abordam cada um destes elementos de forma mais pormenorizada.

([28]) 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, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([29]) Regulamento de Execução (UE) 2024/2690 da Comissão, de 17 de outubro de 2024, que estabelece regras de execução da Diretiva (UE) 2022/2555 relativamente aos requisitos técnicos e metodológicos das medidas de gestão dos riscos de cibersegurança e especifica mais pormenorizadamente os casos em que se considera que um incidente é significativo no que respeita aos prestadores de serviços de DNS, aos registos de nomes de TLD, aos prestadores de serviços de computação em nuvem, aos prestadores de serviços de centro de dados, aos fornecedores de redes de distribuição de conteúdos, aos prestadores de serviços geridos, aos prestadores de serviços de segurança geridos, aos prestadores de serviços de mercados em linha, de motores de pesquisa em linha e de plataformas de serviços de redes sociais e aos prestadores de serviços de confiança (JO L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

8.1.1. *O conceito de «à distância»*

185. O conceito de «à distância» referido no artigo 3.º, ponto 2, é pertinente, mas não suficiente, para determinar se um produto com elementos digitais inclui soluções de tratamento remoto de dados. Além disso, dada a variedade de soluções que este conceito pode abranger, não é possível facultar uma definição exaustiva de «à distância». É necessário que o fabricante proceda a uma avaliação caso a caso.

186. O considerando 11 do Regulamento de Ciber-Resiliência menciona os dados tratados ou armazenados «à distância pelo fabricante», por oposição aos dados tratados ou armazenados «localmente no dispositivo do utilizador». O tratamento remoto de dados habitualmente ocorre fora do ambiente de utilizador de um produto com elementos digitais ou do ambiente operacional de uma organização (para um utilizador profissional). Todavia, tal não impede que o tratamento também se realize perto do dispositivo («na periferia»). A transmissão de dados pode realizar-se por cabo (por exemplo, cabo Ethernet) ou sem fios (por exemplo, Wi-Fi, Bluetooth). A computação em nuvem, incluindo a computação periférica, é um exemplo típico de tratamento de dados efetuado «à distância». Por exemplo, no caso de uma função baseada na nuvem a que o utilizador acede a partir de uma aplicação móvel, parte do tratamento de dados é efetuado na nuvem, fora do ambiente do utilizador.

187. Importa notar que as soluções de tratamento remoto de dados não são necessariamente operadas em infraestruturas de computação em nuvem de terceiros. O tratamento remoto de dados em servidores locais nas instalações do fabricante também pode constituir uma solução de tratamento remoto de dados. Por outras palavras, uma solução executada nas instalações e numa nuvem privada é tão suscetível de se qualificar como solução de tratamento remoto de dados quanto uma solução executada numa nuvem pública e fora das instalações.

188. As duas questões decisivas e cumulativas que determinam se o tratamento de dados é abrangido pelo Regulamento de Ciber-Resiliência enquanto solução de tratamento remoto de dados são apresentadas a seguir, nas secções *8.1.2* e *8.2*. Em caso de resposta afirmativa a ambas as questões, o tratamento remoto de dados qualifica-se como uma solução de tratamento remoto de dados.

8.1.2. *A inexistência desse tratamento de dados impediria o produto com elementos digitais de desempenhar uma das suas funções?*

189. Conforme estabelecido na definição de «tratamento remoto de dados» incluída no artigo 3.º, ponto 2, para que o tratamento de dados à distância se qualifique como uma solução de tratamento remoto de dados, a sua inexistência teria de impedir o produto com elementos digitais de desempenhar uma das suas funções. O conceito de «funções» incluído nesta definição não se limita à «funcionalidade principal» ou à «finalidade prevista» do produto com elementos digitais, pois o Regulamento de Ciber-Resiliência não impõe tal limitação. As funções abrangidas pelo âmbito de aplicação do Regulamento de Ciber-Resiliência são funções que cumprem diretamente a finalidade prevista do produto com elementos digitais, tal como os utilizadores as experienciam, e funções que apoiam o desempenho global do produto.

190. Exemplos de funções em que o tratamento de dados à distância pode ocorrer e que impediriam um produto com elementos digitais de desempenhar uma das suas funções: i) envio de comandos para um dispositivo, ii) sincronização de ficheiros, iii) integração do utilizador, iv) configuração (personalização do produto com elementos digitais), v) distribuição automatizada de atualizações, incluindo atualização de características e correções de segurança, vi) gestão da identidade e do acesso.

191. Em alguns casos, o utilizador pode usar uma função tanto remota como manualmente (por exemplo, ligar ou desligar uma lâmpada com uma aplicação ou manualmente). Esta opção não exclui a qualificação do tratamento de dados associado ao desempenho remoto da função como solução de tratamento remoto de dados. A realização desta função remotamente também é considerada parte das funções que o produto com elementos digitais oferece.

192. Em contrapartida, se a inexistência de um determinado tratamento de dados não impedir o produto com elementos digitais de desempenhar uma das suas funções, esse tratamento não é considerado uma solução de tratamento remoto de dados na aceção do Regulamento de Ciber-Resiliência. Tal inclui, por exemplo, a análise remota de dados de telemetria recolhidos exclusivamente para fins estatísticos ou para o futuro desenvolvimento de produtos.

193. No entanto, mesmo quando o tratamento de dados não suporta uma função de um produto com elementos digitais, poderá ser necessário que os fabricantes tenham em conta se esses componentes remotos introduzem riscos para o produto com elementos digitais no âmbito da sua avaliação dos riscos de cibersegurança (por exemplo, à luz do ambiente operacional do produto) e atenuem esses riscos em conformidade (por exemplo, através de medidas de atenuação a nível do produto).

194. Os sítios Web são um caso específico que merece mais esclarecimentos, conforme explicado na secção *2.1 Colocação no mercado*. Os sítios Web não são abrangidos pelo âmbito das soluções de tratamento remoto de dados se não suportarem uma função de um produto com elementos digitais, como explicado no considerando 11 do Regulamento de Ciber-Resiliência. Para ser considerado abrangido pelo âmbito das soluções de tratamento remoto de dados, não basta que um sítio Web contenha informações sobre um produto com elementos digitais, mesmo que o produto redirecione para esse sítio Web. Por exemplo, o redirecionamento dos utilizadores para uma página Web externa que faculte informações e instruções aos utilizadores não é uma solução de tratamento remoto de dados. Em contrapartida, um sítio Web pode ser abrangido pelo âmbito das soluções de tratamento remoto de dados se permitir ou apoiar uma função de um produto com elementos digitais. Por exemplo, um portal de autenticação que emita credenciais ou fichas necessárias para o funcionamento do produto com elementos digitais seria considerado uma solução de tratamento remoto de dados (desde que os outros critérios da definição também fossem cumpridos).

8.1.3. *O* software *foi concebido e desenvolvido pelo fabricante ou sob a sua responsabilidade?*

195. A definição de «tratamento remoto de dados» constante do artigo 3.º, ponto 2, do Regulamento de Ciber-Resiliência especifica ainda que o *software* desse tratamento de dados à distância tem de ter sido concebido e desenvolvido pelo fabricante ou sob a sua responsabilidade. O tratamento remoto de dados totalmente desenvolvido e concebido pelo fabricante (a nível interno) qualificar-se-ia, naturalmente, como uma solução de tratamento remoto de dados. O mesmo aconteceria se os fabricantes recorressem a um prestador de serviços externo para o desenvolvimento e a conceção de uma solução (ou seja, «sob a sua responsabilidade»). A expressão «sob a sua responsabilidade», isto é, do fabricante, refere-se a soluções de tratamento remoto adaptadas ao fabricante. Trata-se de casos em que o fabricante não se limita a licenciar um produto com elementos digitais ou um serviço existente que um prestador de serviços oferece aos seus clientes ou versões ligeiramente modificadas dos mesmos. «[S]ob a sua responsabilidade» implica que o *software* seja construído exclusivamente pelo fabricante ou em seu nome, com base em projetos e especificações que o mesmo faculta.

196. O conceito de «quem opera a solução» não é um fator decisivo para compreender as soluções de tratamento remoto de dados, pois a definição constante do Regulamento de Ciber-Resiliência refere-se apenas à conceção e ao desenvolvimento dessas soluções. Tal é coerente com a abordagem do Regulamento de Ciber-Resiliência, segundo a qual os requisitos e as obrigações recaem sobre os fabricantes e não sobre o funcionamento do produto com elementos digitais. Se os fabricantes conceberem e desenvolverem soluções que sejam depois operadas por terceiros continuam a ser responsáveis pelo cumprimento dos requisitos essenciais constantes do Regulamento de Ciber-Resiliência para o produto com elementos digitais que colocam no mercado.

197. É necessário distinguir entre os casos em que a conceção e o desenvolvimento são efetuados pelos fabricantes (ou sob a sua responsabilidade) e os casos de recurso a soluções de terceiros não concebidas nem desenvolvidas pelos fabricantes (ou sob a sua responsabilidade). A título de exemplo, é útil ter em conta os modelos de serviços de computação em nuvem mais comuns que proporcionam diferentes graus de controlo pelo utilizador e que também são citados no considerando 12 do Regulamento de Ciber-Resiliência, nomeadamente o *software* como serviço (SaaS, do inglês *Software as a Service*), a plataforma como serviço (PaaS, do inglês *Platform as a Service*) e as infraestruturas como serviço (IaaS, do inglês *Infrastructure as a Service*).

198. No caso de uma solução de IaaS de terceiros, o fabricante não gere nem controla os recursos físicos e virtuais subjacentes (como o *hardware* subjacente e o hipervisor do prestador de serviços de computação em nuvem), mas tem a capacidade de implantar e executar *software* arbitrário utilizando esses recursos, como sistemas operativos e aplicações. Esse *software* é concebido e desenvolvido pelo fabricante, ou sob a sua responsabilidade, e pode, por conseguinte, qualificar-se como uma solução de tratamento remoto de dados (se preencher os outros critérios da definição).

199. No caso de uma solução de PaaS de terceiros, o fabricante implanta a sua própria aplicação (criada ou adquirida) utilizando linguagens de programação e ambientes de execução disponibilizados pelo prestador de serviços de computação em nuvem, bem como integra a aplicação no seu produto com elementos digitais. O fabricante tem controlo sobre a aplicação e, eventualmente, sobre as definições de configuração para o ambiente de execução. Por conseguinte, a aplicação é concebida e desenvolvida pelo fabricante, ou sob a sua responsabilidade, e pode, portanto, qualificar-se como uma solução de tratamento remoto de dados (se preencher os outros critérios da definição).

200. No caso de uma solução de SaaS de terceiros, o fornecedor de SaaS disponibiliza ao fabricante uma aplicação plenamente desenvolvida para ser integrada no seu produto com elementos digitais. O fabricante tem uma capacidade limitada para gerir as definições de configuração da aplicação específicas do utilizador. Por conseguinte, a aplicação não foi concebida nem desenvolvida pelo fabricante, nem está sob a sua responsabilidade.

201. Todavia, caso determinados elementos não se qualifiquem como soluções de tratamento remoto de dados (por exemplo, o hipervisor, no caso de IaaS de terceiros, o sistema operativo, no caso de uma solução de PaaS de terceiros, ou a aplicação de SaaS de terceiros), mas forem integrados no produto com elementos digitais de uma forma que afete a sua segurança, essas soluções devem ser consideradas semelhantes a componentes de terceiros. O fabricante é obrigado a identificar e avaliar os riscos associados à integração desses elementos, bem como a dar-lhes resposta aplicando os requisitos essenciais ao próprio produto com elementos digitais. Se for caso disso, tal pode ser apoiado pelas funções de segurança disponibilizadas pelo prestador de serviços de computação em nuvem através do seu modelo de responsabilidade partilhada, em que o fabricante utiliza ou configura essas funções para dar resposta aos riscos identificados. Além disso, o fabricante deverá cumprir uma obrigação semelhante à de exercer a diligência devida referida no artigo 13.º, n.º 5, relacionada com a segurança destes componentes, de forma proporcionada ao risco que a solução remota representa para a segurança do produto com elementos digitais.

202. Portanto, resumindo:

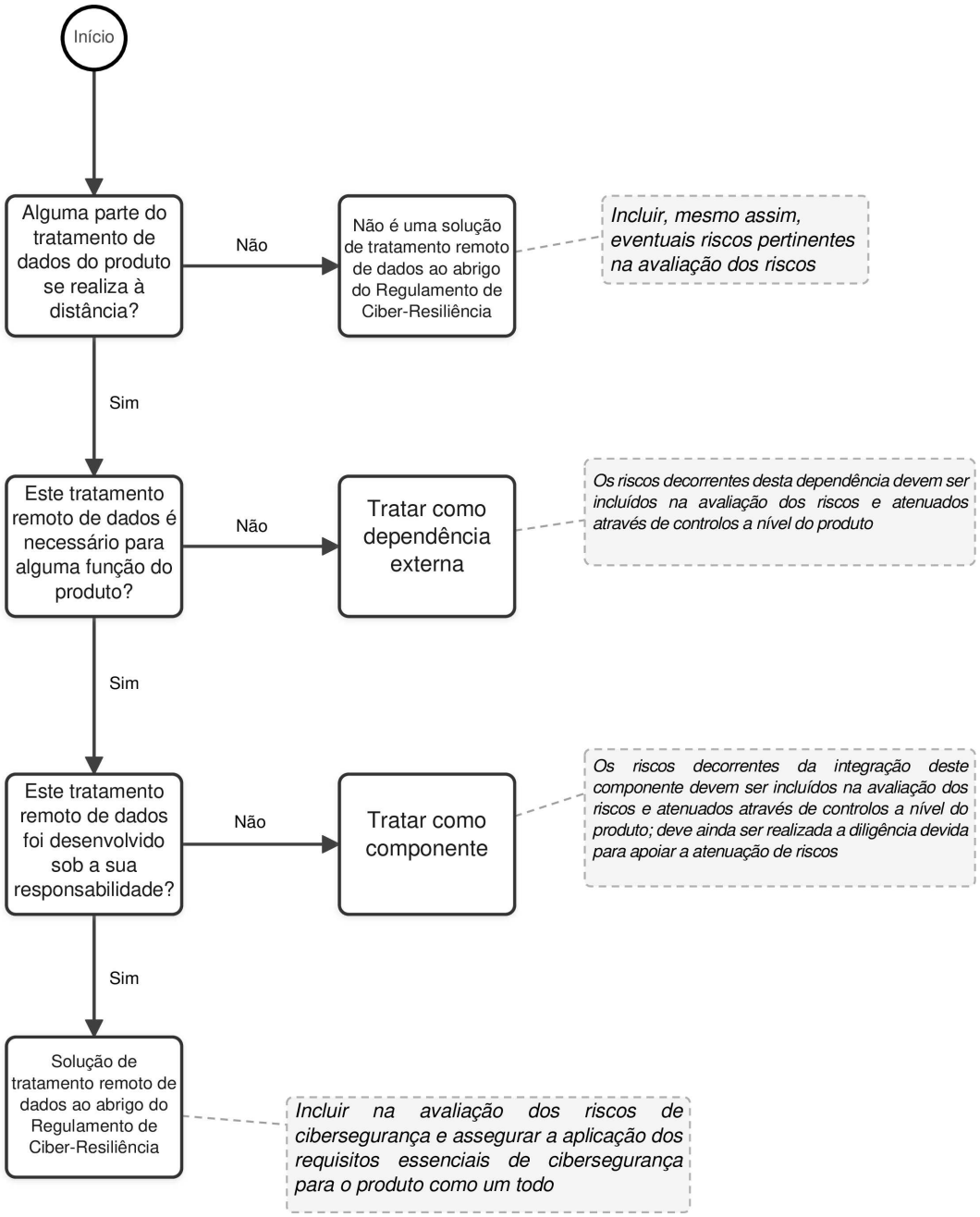
a) Para que o tratamento de dados se qualifique como uma solução de tratamento remoto de dados, a resposta a ambas as perguntas colocadas nas secções *8.1.2 A inexistência desse tratamento de dados impediria o produto com elementos digitais de desempenhar uma das suas funções?* e *8.1.3 O software foi concebido e desenvolvido pelo fabricante ou sob a sua responsabilidade?* tem de ser afirmativa;

b) Se a resposta à pergunta da secção *8.1.2 A inexistência desse tratamento de dados impediria o produto com elementos digitais de desempenhar uma das suas funções?* for negativa, os fabricantes devem avaliar os riscos decorrentes da existência desse tratamento de dados no âmbito da sua avaliação dos riscos;

c) Se a resposta à pergunta da secção *8.1.2 A inexistência desse tratamento de dados impediria o produto com elementos digitais de desempenhar uma das suas funções?* for afirmativa, mas a resposta à pergunta em *8.1.3 O software foi concebido e desenvolvido pelo fabricante ou sob a sua responsabilidade?* for negativa, os fabricantes devem tratar a solução de terceiros como um componente. No âmbito da avaliação dos riscos, os fabricantes devem avaliar os riscos decorrentes da integração dessa solução e atenuá-los em conformidade. Além disso, os fabricantes devem exercer a diligência devida.

Figura 9:

Fluxograma estilizado para determinar se um produto com elementos digitais contém soluções de tratamento remoto de dados



8.2. Implicações práticas e técnicas das soluções de tratamento remoto de dados e recurso a soluções de terceiros

203. O Regulamento de Ciber-Resiliência segue uma abordagem baseada no risco, consagrada no artigo 13.º, n.os 2 e 3, bem como no primeiro requisito essencial constante da parte I do anexo I, segundo o qual «[o]s produtos com elementos digitais devem ser concebidos, desenvolvidos e produzidos de modo a garantir um nível adequado de cibersegurança com base nos riscos». Por conseguinte, ao aplicar os requisitos do Regulamento de Ciber-Resiliência à solução de tratamento remoto de dados e ao tratamento dos riscos decorrentes de serviços de terceiros integrados no produto com elementos digitais, deve ser tida em conta uma abordagem baseada no risco.

204. Em primeiro lugar, os fabricantes devem i) indicar na documentação técnica que o seu produto com elementos digitais possui uma solução de tratamento remoto de dados ou recorre a soluções remotas de terceiros e ii) descrever essas soluções. Se a mesma solução de tratamento remoto de dados apoiar vários produtos com elementos digitais, a solução de tratamento remoto de dados tem de ser declarada na documentação técnica de cada produto. A documentação relativa às soluções de tratamento remoto de dados que servem vários produtos com elementos digitais pode ser reutilizada de uma avaliação da conformidade do produto para outra.

205. Conforme indicado no considerando 11, as soluções de tratamento remoto de dados que fazem parte do produto com elementos digitais, e que, por conseguinte, estão sujeitas à avaliação da conformidade do produto, devem limitar-se aos módulos de *software* responsáveis pela funcionalidade do produto com elementos digitais e às interfaces que esses módulos utilizam com serviços externos. Não se consideram como soluções de tratamento remoto de dados outros sistemas de retaguarda que realizem tratamentos subsequentes e com os quais o produto com elementos digitais não interaja diretamente.

206. No entanto, esses sistemas de retaguarda continuam a constituir dependências externas que devem ser apreciadas no âmbito da avaliação dos riscos de cibersegurança e atenuadas através de medidas a nível dos produtos. Com efeito, a avaliação dos riscos realizada pelo fabricante deve ter em conta: i) riscos relacionados com soluções de tratamento remoto de dados, ii) riscos relacionados com o recurso a soluções remotas de terceiros (semelhantes a componentes de terceiros) e iii) riscos relacionados com o ambiente do produto (por exemplo, *hardware* subjacente). Os fabricantes devem aplicar controlos de segurança ao próprio produto com elementos digitais para atenuar esses riscos.

207. Além disso, no âmbito da avaliação da conformidade e/ou do cumprimento das obrigações de diligência devida relacionadas com serviços remotos de terceiros, é possível reutilizar a seguinte lista não exaustiva de mecanismos de garantia para apoiar a avaliação do fabricante:

a) Provas do cumprimento das obrigações previstas no Regulamento de Execução (UE) 2024/2690 da Comissão;

b) Provas do cumprimento das obrigações previstas no Regulamento (UE) 2022/2554 (Regulamento DORA);

c) Declaração de conformidade ou certificado obtido ao abrigo de um sistema europeu de certificação da cibersegurança [adotado nos termos do Regulamento (UE) 2019/881 (Regulamento Cibersegurança)];

d) Provas da conformidade com as normas ISO/IEC 27017:2015 ou ISO/IEC 27001:2022.

208. Por último, nas suas interações com terceiros prestadores de serviços remotos, os fabricantes têm de aplicar as medidas de segurança mais adequadas com base na sua avaliação dos riscos (e, se for caso disso, apoiadas pelo modelo de responsabilidade partilhada do prestador). Essas medidas de atenuação devem incluir controlos de segurança para os seus produtos com elementos digitais e a verificação das medidas de segurança facultadas pelos próprios terceiros prestadores de serviços (diligência devida). Um instrumento para atenuar esses riscos pode consistir na integração de garantias de segurança nos respetivos acordos de nível de serviço (ANS) com terceiros prestadores de serviços, incluindo garantias de que os prestadores tratam adequadamente as vulnerabilidades. Uma alteração importante das soluções disponibilizadas pelos terceiros prestadores de serviços remotos não deve ser considerada uma modificação substancial do produto com elementos digitais, pois estes elementos não são da responsabilidade do fabricante. Todavia, no âmbito das suas obrigações em matéria de diligência devida e para atenuar corretamente os riscos decorrentes do recurso a terceiros prestadores de serviços, os fabricantes são incentivados a assegurar que os seus terceiros prestadores de serviços de computação em nuvem os mantêm devidamente informados sobre as alterações que aplicam às suas soluções. Com base nessas informações, os fabricantes podem ter de rever a sua avaliação dos riscos. A avaliação dos riscos atualizada deve ter em conta se os terceiros prestadores de serviços continuam a oferecer garantias suficientes em termos de cibersegurança e se os controlos de segurança a nível dos produtos continuam a ser adequados. Em alguns casos, os fabricantes podem ter de modificar esses controlos ou mudar de terceiros prestadores de serviços.

8.3. **Casos de utilização para soluções de tratamento remoto de dados**

A fim de facultar orientações práticas adicionais aos fabricantes, a presente secção introduz uma série de casos de utilização fictícios, descrevendo produtos com elementos digitais arquetípicos que recorrem ao tratamento remoto de dados e ilustrando se esse tratamento se qualifica como uma solução de tratamento remoto de dados na aceção do Regulamento de Ciber-Resiliência.

8.3.1. *Aplicação bancária móvel*

Uma entidade financeira coloca uma aplicação bancária móvel no mercado. Os sistemas de retaguarda da aplicação apoiam, nomeadamente, a autenticação, a autorização, a gestão de contas e os pagamentos. A entidade financeira utiliza uma estratégia híbrida assente em infraestruturas internas, bem como em soluções remotas de terceiros para apoiar as funcionalidades da aplicação. Inclui-se:

Infraestrutura autoalojada desenvolvida pela entidade financeira:

— O cliente abre a aplicação bancária móvel e é autenticado através da interface bancária, uma solução autoalojada desenvolvida pela entidade financeira que recebe os pedidos da aplicação e devolve as respostas correspondentes. A interface bancária verifica a identidade do cliente consultando o sistema de gestão de contas e concede acesso à aplicação.

— O cliente inicia a transferência através da aplicação. A aplicação transmite a instrução à interface bancária, que apresenta um pedido correspondente ao sistema de livro-razão.

— O sistema de gestão de contas e o sistema de livro-razão, ambos autoalojados, mas logicamente separados da interface bancária, registam a transação.

— O sistema de livro-razão devolve o estado da transação à interface bancária, que apresenta o resultado ao cliente.

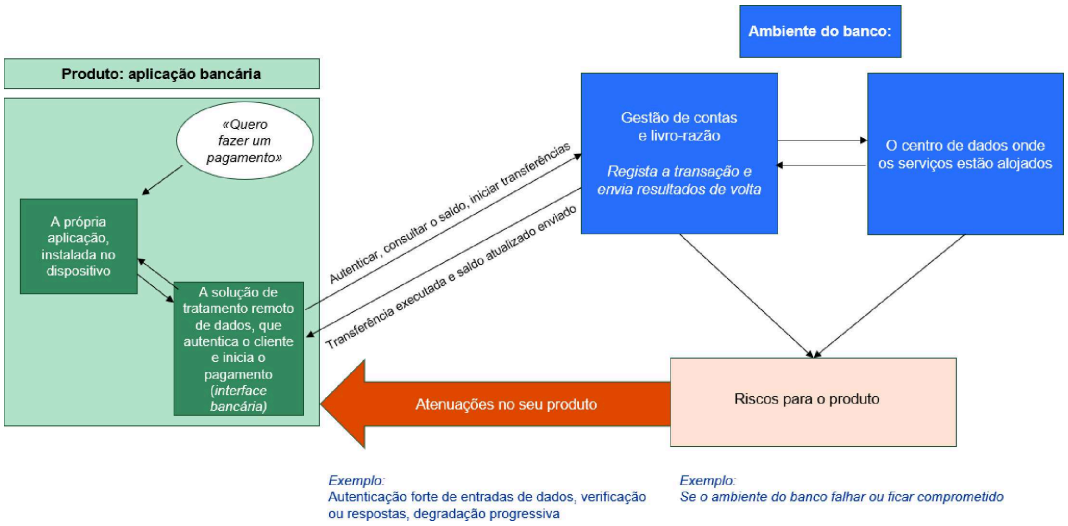
Implicações para soluções de tratamento remoto de dados:

— A interface bancária é necessária para que a aplicação desempenhe as suas funções, nomeadamente autenticar o cliente, enviar as instruções do cliente, incluindo as instruções de pagamento e transferência, e devolver o estado resultante. A interface bancária é concebida e desenvolvida sob a responsabilidade do fabricante. Uma vez que a resposta a ambas as perguntas apresentadas nas secções anteriores é afirmativa, a interface bancária deve ser considerada uma solução de tratamento remoto de dados. Por conseguinte, deve ser incluída na avaliação dos riscos de cibersegurança e na aplicação dos requisitos essenciais para o produto com elementos digitais no seu todo. O tratamento subsequente de uma instrução, depois de ser apresentada, em especial o registo da transação nos sistemas de gestão de contas e de livro-razão, a liquidação e a compensação, é efetuado por sistemas com os quais a aplicação não interage diretamente e não constitui, a esse título, uma solução de tratamento remoto de dados.

— O sistema de gestão de contas e o sistema de livro-razão não se qualificam como soluções de tratamento remoto de dados para a aplicação bancária. A aplicação não interage diretamente com esses sistemas (interagindo, em vez disso, com a interface bancária, a qual, por sua vez, recorre aos mesmos). Embora a sua disponibilidade possa ser necessária para a execução de uma função, o Regulamento de Ciber-Resiliência abrange apenas as partes do sistema que interagem diretamente com o produto com elementos digitais. Por conseguinte, não são abrangidos pela definição de soluções de tratamento remoto de dados para efeitos do Regulamento de Ciber-Resiliência. No entanto, esses sistemas continuam a ser dependências externas que podem dar origem a riscos de cibersegurança significativos para o produto com elementos digitais. Por exemplo, o comprometimento do sistema de livro-razão pode permitir que um atacante influencie os resultados das transações que são posteriormente apresentados na aplicação. Por conseguinte, o fabricante é obrigado a identificar e avaliar esses riscos no âmbito da avaliação dos riscos de cibersegurança e a atenuá-los através de medidas a nível do produto, como a autenticação forte das interfaces de retaguarda, a proteção da integridade dos dados de transações, canais de comunicação seguros e a verificação das respostas que a aplicação recebe.

Figura 10:

Representação estilizada de uma aplicação bancária que recorre a soluções de tratamento remoto de dados



SaaS de terceiros para apoio ao cliente:

— A entidade financeira integra na sua aplicação uma solução de espaço de conversa para efeitos de apoio ao cliente, desenvolvida e gerida por um terceiro prestador de serviços; o terceiro prestador de serviços escreveu o código do servidor do espaço de conversa, construiu a interface do utilizador e gere a infraestrutura onde o espaço de conversa está implantado (ou seja, o modelo de SaaS).

— Quando o cliente inicia um pedido de apoio, a aplicação estabelece a ligação entre o cliente e o serviço de terceiros para criar uma sessão de conversa e gerir o fluxo de mensagens, sem proporcionar ao terceiro acesso aos sistemas bancários principais.

Implicações para soluções de tratamento remoto de dados:

— A solução de espaço de conversa para apoio é necessária para que o produto com elementos digitais desempenhe uma das suas funções, mas não é concebida nem desenvolvida pela entidade financeira ou sob a sua responsabilidade. Por conseguinte, não se trata de uma solução de tratamento remoto de dados. No entanto, deve ser tratada como um componente de terceiros. O recurso a esse serviço de terceiros pode criar riscos de cibersegurança para a aplicação bancária, por exemplo, se um atacante utilizar o canal de conversa para usurpar a identidade do banco ou apresentar conteúdos maliciosos aos utilizadores. Na sua avaliação dos riscos de cibersegurança, a entidade financeira deve ter em conta esses riscos e atenuá-los através de medidas a nível do produto, como o isolamento da função de conversa em relação às funcionalidades bancárias principais, o controlo dos fluxos de dados e a validação de conteúdos. Também deve ser exercida a diligência devida em relação ao SaaS.

8.3.2. *Termóstato inteligente*

Um termóstato inteligente permite aos utilizadores controlar a temperatura das suas casas através de uma aplicação móvel. A aplicação móvel e o termóstato inteligente recorrem ao tratamento remoto de dados para proceder ao intercâmbio de dados (por exemplo, pedido de aumento da temperatura) e ao armazenamento de dados (por exemplo, preferências dos utilizadores). Estas funções foram desenvolvidas e concebidas sob a responsabilidade do fabricante, mas são executadas numa infraestrutura física e virtual subjacente disponibilizada por um terceiro (IaaS de terceiros).

Tendo em conta que o termóstato inteligente não seria capaz de desempenhar as suas funcionalidades inteligentes sem este tratamento remoto de dados, a sua inexistência impediria o produto com elementos digitais de desempenhar uma ou mais das suas funções. Além disso, o *software* foi desenvolvido e concebido sob a responsabilidade do fabricante do termóstato inteligente. Por conseguinte, o tratamento remoto de dados qualifica-se como solução de tratamento remoto de dados, nos termos da definição constante do Regulamento de Ciber-Resiliência.

Para efeitos de conformidade com o Regulamento de Ciber-Resiliência, o fabricante do termóstato inteligente tem de documentar, na documentação técnica do produto com elementos digitais, a solução de tratamento remoto de dados, bem como o recurso ao sistema de IaaS de terceiros, incluindo informações pormenorizadas sobre o serviço contratado. Na avaliação dos riscos, o fabricante deve ter em conta esses elementos, incluindo a finalidade prevista e a utilização razoavelmente previsível do produto com elementos digitais. O fabricante aplica os requisitos essenciais constantes do Regulamento de Ciber-Resiliência com base nos riscos associados à solução de tratamento remoto de dados. No caso do sistema de IaaS de terceiros, o fabricante deve assegurar que as medidas de segurança facultadas pelo terceiro prestador de serviços são adequadas e/ou tomar medidas pertinentes em relação à infraestrutura. No primeiro caso, o fabricante poderia, por exemplo, solicitar provas do cumprimento das obrigações decorrentes da Diretiva SRI 2.

8.3.3. *Leitor de livros digitais*

O fabricante do *software* de um leitor de livros digitais utiliza um serviço de armazenamento SaaS de terceiros para armazenar livros digitais adquiridos pelos clientes e permitir-lhes aceder aos seus livros. A inexistência deste serviço de armazenamento impediria o produto com elementos digitais de desempenhar uma das suas funções, mas o serviço de armazenamento SaaS de terceiros não é desenvolvido pelo fabricante ou sob a sua responsabilidade. O prestador do SaaS disponibiliza-o aos clientes para qualquer caso de utilização.

O serviço de armazenamento SaaS não corresponde à definição de solução de tratamento remoto de dados. No entanto, o fabricante do leitor de livros digitais recorre a esse serviço externo para o funcionamento do seu produto com elementos digitais e, por conseguinte, na sua avaliação dos riscos de cibersegurança deve ter em conta os riscos associados. O fabricante do leitor de livros digitais deve tratar o SaaS como um componente. O fabricante deve aplicar medidas de segurança adequadas a nível do produto, como autenticação segura, cifragem e proteção da integridade das comunicações com o serviço de armazenamento. A diligência devida ao selecionar e integrar o prestador de SaaS apoiará igualmente as obrigações do fabricante, para que o produto com elementos digitais no seu todo possa cumprir os requisitos essenciais.

8.3.4. *Robô industrial*

Um robô industrial tem a tarefa de recolher peças. O robô envia informações recolhidas através de câmaras para um serviço remoto concebido e desenvolvido pelo fabricante. Este serviço é executado numa infraestrutura física e virtual subjacente disponibilizada por um terceiro prestador de serviços (IaaS de terceiros). O serviço de computação em nuvem calcula a posição de uma peça com base nas imagens recebidas da câmara e envia comandos de volta ao robô para recolher as peças.

A inexistência deste tratamento de dados impediria o robô industrial de recolher peças e, por conseguinte, de desempenhar uma das suas funções. Além disso, o *software* executado sobre a infraestrutura subjacente foi concebido e desenvolvido pelo fabricante. O *software* concebido e desenvolvido pelo fabricante corresponde à definição de solução de tratamento remoto de dados.

O fabricante do robô industrial tem de documentar, na documentação técnica do produto com elementos digitais, a solução de tratamento remoto de dados, bem como o recurso ao sistema de IaaS de terceiros (incluindo informações pormenorizadas sobre o serviço contratado). O fabricante também tem de ter em conta esses elementos na avaliação dos riscos, incluindo a finalidade prevista e a utilização razoavelmente previsível do produto com elementos digitais. O fabricante aplica os requisitos essenciais constantes do Regulamento de Ciber-Resiliência ao produto com elementos digitais, incluindo a respetiva solução de tratamento remoto de dados, com base nos riscos. A diligência devida ao selecionar o prestador de IaaS apoiará igualmente as obrigações do fabricante. Por exemplo, o fabricante pode solicitar provas do cumprimento das obrigações decorrentes da Diretiva SRI 2.

8.3.5. *Rede celular*

Um telemóvel inteligente recorre a uma rede 5G para proporcionar ligação à Internet, chamadas telefónicas e mensagens aos seus utilizadores (conectividade móvel). A rede celular é desenvolvida e concebida por operadores de telecomunicações. A rede inclui pequenas células e torres de telecomunicações móveis, bem como outros equipamentos de rede.

O produto com elementos digitais deve poder ligar-se corretamente a uma rede, sendo esta uma das suas funções. Todavia, o facto de essa rede estar ou não em funcionamento é irrelevante para determinar se o produto com elementos digitais está a funcionar corretamente. A rede é apenas um canal de comunicação e não é necessária para que o produto com elementos digitais desempenhe a sua função de «ligar-se corretamente a uma rede». Do mesmo modo, um cabo Ethernet, um encaminhador ou um sinal Wi-Fi não é considerado tratamento de dados cuja inexistência impediria o produto com elementos digitais de desempenhar uma das suas funções, mas sim um facilitador de comunicação/conectividade.

Por conseguinte, a rede celular não corresponde à definição de solução de tratamento remoto de dados. Não deve considerar-se a rede como sendo um componente de terceiros, pois não existe *software* integrado no produto com elementos digitais, em vez disso o produto apenas recorre a esta rede. Como tal, não é necessário que o fabricante exerça obrigações de diligência devida em relação ao fornecedor de rede.

9. **ELEMENTOS ADICIONAIS**

9.1. **Obrigações em matéria de comunicação de informações**

209. Nos termos do artigo 14.º, n.ºs 1 e 3, do Regulamento de Ciber-Resiliência, o fabricante é obrigado a notificar simultaneamente a CSIRT designada coordenadora e a ENISA de i) qualquer vulnerabilidade ativamente explorada existente no seu produto com elementos digitais de que tome conhecimento e de ii) qualquer incidente grave com impacto na segurança do produto com elementos digitais de que tome conhecimento.

210. Em conformidade com o artigo 69.º, n.º 3, e com o artigo 71.º, n.º 2, segunda frase, a obrigação de cumprir o artigo 14.º é aplicável a partir de 11 de setembro de 2026 a todos os produtos com elementos digitais abrangidos pelo âmbito de aplicação do Regulamento de Ciber-Resiliência, incluindo os produtos com elementos digitais colocados no mercado antes de 11 de dezembro de 2027. Além disso, ao contrário das obrigações de tratamento de vulnerabilidades, que se mantêm apenas durante o período de apoio de um produto, as obrigações em matéria de comunicação de informações continuam a aplicar-se depois de um produto com elementos digitais deixar de ser objeto de apoio. Se um produto com elementos digitais tiver sido colocado no mercado antes de 11 de dezembro de 2027, ou se o seu período de apoio tiver terminado, o fabricante não é obrigado a cumprir as obrigações de tratamento de vulnerabilidades estabelecidas na parte II do anexo I.

211. Importa recordar que a obrigação de notificar esses eventos se aplica quando o fabricante toma conhecimento de que uma vulnerabilidade está a ser ativamente explorada ou de que ocorreu um incidente grave que comprometeu a segurança do seu produto com elementos digitais. Por conseguinte, as orientações sobre quando se considera que um fabricante tomou conhecimento devem ajudar os fabricantes a determinar o momento em que começam os prazos aplicáveis de comunicação de informações.

212. Os fabricantes podem estar sujeitos a obrigações em matéria de comunicação de informações comparáveis por força de diferentes atos da UE. A fim de assegurar que o conceito de «tomar conhecimento» é interpretado de forma coerente e de facilitar o cumprimento dessas obrigações pelos fabricantes, as presentes orientações estão em consonância com o considerando 31 do Regulamento de Execução (UE) 2024/2690 da Comissão e com a secção II, ponto A, das Orientações n.º 9/2022 sobre a notificação da violação de dados pessoais ao abrigo do Regulamento Geral sobre a Proteção de Dados (RGPD).

213. Em alguns casos, um fabricante detetará um evento suspeito, ou um terceiro — como uma pessoa, um cliente, uma entidade, uma autoridade, um órgão de comunicação social ou outra fonte — chamará a sua atenção para um potencial incidente ou vulnerabilidade. Nesses casos, o fabricante deve avaliar imediatamente o evento suspeito para determinar se constitui uma vulnerabilidade ativamente explorada ou um incidente grave com impacto na segurança do produto com elementos digitais. Por conseguinte, deve considerar-se que o fabricante tomou conhecimento quando, após essa avaliação inicial, tem um grau razoável de certeza de que: i) uma vulnerabilidade existente no seu produto com elementos digitais está a ser ativamente explorada ou ii) ocorreu um incidente grave que comprometeu a segurança do seu produto com elementos digitais.

214. Por conseguinte, o momento em que se pode considerar que um fabricante tomou conhecimento dependerá das circunstâncias da vulnerabilidade ativamente explorada específica ou do incidente grave específico. Em alguns casos, será relativamente evidente, desde o início, que uma vulnerabilidade está a ser ativamente explorada ou que um incidente grave tem impacto na segurança de um produto com elementos digitais. Noutros casos, pode demorar algum tempo a determinar se um produto com elementos digitais é afetado por uma vulnerabilidade e se essa vulnerabilidade está a ser explorada por um interveniente mal-intencionado, ou se um incidente está a afetar a segurança de um produto com elementos digitais. Contudo, a tónica deve ser colocada numa ação rápida para realizar a avaliação inicial, a fim de determinar se essas condições estão efetivamente preenchidas, em especial quando a vulnerabilidade seja suscetível de representar um risco significativo, e, em caso afirmativo, tomar medidas corretivas e proceder à notificação em conformidade com o Regulamento de Ciber-Resiliência.

215. Além disso, a estrutura das obrigações em matéria de comunicação de informações exige que os fabricantes atualizem progressivamente as suas notificações, à medida que as suas investigações internas avançam e que o seu conhecimento da vulnerabilidade ativamente explorada ou do incidente se torna mais pormenorizado. Em especial, os fabricantes são obrigados a apresentar uma notificação de alerta precoce com informações limitadas sem demora injustificada e, em qualquer caso, no prazo de 24 horas após terem tomado conhecimento. Posteriormente, são necessárias informações adicionais no âmbito da notificação, a apresentar sem demora injustificada e, em qualquer caso, no prazo de 72 horas após terem tomado conhecimento («notificação de 72 horas»). O relatório completo deve ser apresentado no prazo de 14 dias após a disponibilização de uma medida corretiva ou de atenuação, no caso de vulnerabilidades ativamente exploradas, ou no prazo de um mês após a notificação de 72 horas, no caso de incidentes graves.

216. Conforme também recordado na secção *3.3.1 Apoio contínuo e garantia da viabilidade do* SL/A, os administradores de *software* de código-fonte aberto são igualmente obrigados a comunicar vulnerabilidades ativamente exploradas, por força do artigo 24.º, n.º 3 ([30]). Essa obrigação aplica-se quando se toma conhecimento de uma vulnerabilidade ativamente explorada, e não apenas quando existe uma vulnerabilidade na base de códigos de um SL/A para o qual essa entidade é um administrador. Na prática, uma vez que os componentes do SL/A são normalmente integrados a jusante noutros produtos com elementos digitais, é provável que um administrador tome conhecimento da exploração ativa através de relatórios de terceiros, que identificam a exploração em componentes do SL/A como integrada noutros produtos com elementos digitais. Pode ser o caso, por exemplo, quando um fabricante de um produto com elementos digitais deteta a exploração ativa num componente do SL/A integrado no seu próprio produto e a comunica ao administrador desse componente, ou quando um utilizador ou um investigador no domínio da segurança encontra provas de exploração de um componente do SL/A integrado num produto com elementos digitais e comunica essa exploração ativa ao administrador do componente.

217. Importa igualmente clarificar que, dado que a obrigação de comunicar vulnerabilidades ativamente exploradas se aplica quando o fabricante toma conhecimento de exploração ativa, o fabricante não é obrigado a comunicar vulnerabilidades de cuja exploração ativa já teve conhecimento antes de 11 de setembro de 2026 (data em que a obrigação em matéria de comunicação de informações começa a aplicar-se). Por conseguinte, o Regulamento de Ciber-Resiliência não exige a comunicação retroativa dessas vulnerabilidades. Em contrapartida, a obrigação é aplicável caso o fabricante tenha tido conhecimento de uma vulnerabilidade antes de 11 de setembro de 2026, mas, nessa altura, não tinha conhecimento de qualquer exploração ativa da mesma (quer porque ainda não tinha ocorrido, quer porque o fabricante não tinha tido conhecimento da mesma). Se, após 11 de setembro de 2026, ocorrer posteriormente uma exploração ativa ou o fabricante tomar conhecimento da mesma, a vulnerabilidade é considerada ativamente explorada, sujeita à obrigação em matéria de comunicação de informações.

218. Do mesmo modo, um fabricante só é obrigado a comunicar vulnerabilidades ativamente exploradas contidas no seu produto com elementos digitais. Caso um produto com elementos digitais contenha uma vulnerabilidade ativamente explorada proveniente de um componente de terceiros, o fabricante do produto com elementos digitais é obrigado a notificar essa vulnerabilidade ativamente explorada. No entanto, se um fabricante tiver conhecimento de que um componente de terceiros contém uma vulnerabilidade, mas essa vulnerabilidade i) não puder ser explorada no seu produto com elementos digitais (por exemplo, porque o código vulnerável não está acessível) ou ii) não tiver sido explorada no seu produto com elementos digitais, essa vulnerabilidade não é considerada uma vulnerabilidade ativamente explorada existente no seu produto com elementos digitais e, por conseguinte, não está sujeita à comunicação obrigatória por parte desse fabricante. Esse fabricante continua a poder notificar essa vulnerabilidade a título voluntário, em conformidade com o artigo 15.º do Regulamento de Ciber-Resiliência. É igualmente obrigado a cumprir os requisitos de tratamento de vulnerabilidades previstos na parte II do anexo I do Regulamento de Ciber-Resiliência, bem como a comunicar a vulnerabilidade à pessoa ou entidade que fabrica ou mantém o componente, por força do artigo 13.º, n.º 6, e conforme explicado mais pormenorizadamente na secção *9.2.1 Comunicação de informações a montante e* partilha de correções de segurança.

([30]) Na medida em que o administrador esteja envolvido no desenvolvimento de um produto com elementos digitais.

219. Após terem tomado conhecimento de uma vulnerabilidade ativamente explorada ou de um incidente grave, os fabricantes são igualmente obrigados, por força do artigo 14.º, n.º 8, a informar os utilizadores afetados e, se for caso disso, todos os utilizadores. Caso não o façam em tempo útil, as CSIRT que receberam a notificação podem facultar essas informações aos utilizadores, quando tal for considerado proporcionado e necessário para prevenir ou atenuar o impacto dessa vulnerabilidade ou incidente.

220. Em consonância com a abordagem baseada no risco constante do Regulamento de Ciber-Resiliência, a obrigação de informar os utilizadores prevista no artigo 14.º, n.º 8, deve ser aplicada de forma proporcionada e baseada no risco. Em especial, a prestação de informações sobre uma vulnerabilidade ativamente explorada ou um incidente grave não implica que essas informações devam ser tornadas públicas ou divulgadas indiscriminadamente. Se for caso disso, e tendo em conta a natureza do produto com elementos digitais, os utilizadores afetados e a vulnerabilidade ou o potencial impacto do incidente, os fabricantes podem limitar a divulgação de informações pormenorizadas aos utilizadores pertinentes ou aos clientes em causa. É o caso, em especial, de produtos com elementos digitais utilizados em ambientes sensíveis ou essenciais, em que a divulgação pública de pormenores técnicos pode, por si só, aumentar os riscos de cibersegurança ou facilitar uma maior exploração.

221. Depois de a vulnerabilidade ter sido devidamente resolvida ou atenuada, pode ser adequada uma divulgação mais ampla. Será o caso, por exemplo, se a divulgação contribuir para aumentar a sensibilização geral ou permitir aos utilizadores verificar se os seus produtos com elementos digitais deixaram de ser afetados. Nesses casos, o nível de pormenor e o calendário de qualquer divulgação mais ampla deverão continuar a ser proporcionados e a ter em conta os riscos residuais de exploração, a natureza do produto com elementos digitais e os interesses dos utilizadores em causa. Além disso, a parte II, ponto 4, do anexo I exige que os fabricantes divulguem publicamente informações sobre as vulnerabilidades corrigidas, uma vez disponibilizada uma atualização de segurança.

9.2. **Tratamento de vulnerabilidades**

9.2.1. *Comunicação de informações a montante e partilha de correções de segurança*

222. O artigo 13.º, n.º 6, do Regulamento de Ciber-Resiliência exige que os fabricantes comuniquem vulnerabilidades em componentes integrados à pessoa ou entidade que fabrica ou mantém esse componente («comunicação de informações a montante»).

223. Os fabricantes são obrigados a comunicar informações a montante apenas no que diz respeito à versão do componente que integram. Se a pessoa ou entidade que fabrica ou mantém o componente tiver estabelecido políticas de segurança, processos de divulgação coordenada de vulnerabilidades ou canais designados para a comunicação de vulnerabilidades, os fabricantes deverão comunicar as vulnerabilidades em conformidade com os mesmos, em especial caso a divulgação prematura de vulnerabilidades não corrigidas possa aumentar os riscos de cibersegurança. Além disso, a fim de reduzir os encargos para os responsáveis pela manutenção a montante, em especial em projetos de fonte aberta, os fabricantes não são obrigados a comunicar informações a montante se puderem confirmar que a pessoa ou entidade que fabrica ou mantém um componente tem conhecimento da existência de uma vulnerabilidade. Incentiva-se os fabricantes a tomarem medidas razoáveis para evitar a apresentação de relatórios duplicados, por exemplo, através da verificação de bases de dados de vulnerabilidades acessíveis ao público, avisos de segurança específicos por projeto ou mecanismos de acompanhamento de problemas criados antes da comunicação de informações a montante.

224. Os fabricantes são obrigados a comunicar a montante apenas as vulnerabilidades que existem no próprio componente integrado, e não as vulnerabilidades que existem em resultado da integração entre o componente e outro código desenvolvido pelo fabricante ou da integração de outros componentes. Todavia, pode haver situações em que a integração de um componente num produto com elementos digitais específico revele determinados comportamentos, interações ou características pertinentes para a segurança desse componente que não eram evidentes, ou que não eram facilmente identificáveis, isoladamente. Nesses casos, incentiva-se os fabricantes a comunicarem estas informações à pessoa ou entidade que fabrica ou mantém o componente, a fim de promover boas práticas de tratamento de vulnerabilidades destinadas a facilitar uma reparação eficaz e a melhorar a segurança global do ecossistema de componentes.

225. Por último, os fabricantes também não são obrigados a comunicar a vulnerabilidade a montante se o componente já não dispuser de um responsável pela manutenção ou se o fabricante já não recorrer ao responsável pela manutenção original para novas versões ou correções de segurança. Nesses casos, no entanto, incentiva-se o fabricante a informar os utilizadores desse componente através de medidas alternativas razoáveis, por exemplo, por meio dos mecanismos comunitários existentes (como listas de endereços ou emissão de bilhetes) ou de registos públicos de vulnerabilidade.

226. Além disso, nos termos do artigo 13.º, n.º 6, os fabricantes que tenham desenvolvido uma modificação do *software* para dar resposta a uma vulnerabilidade num componente integrado são obrigados a partilhar essa modificação do *software* («correção de segurança») com a pessoa ou entidade que fabrica ou mantém o componente («partilha a montante»).

227. Caso os fabricantes sejam obrigados a partilhar uma correção de segurança por força do artigo 13.º, n.º 6, essa correção deve, se for caso disso, ser facultada num formato legível por máquina, de uma forma que possa ser facilmente verificada e, se pertinente, integrada pela pessoa ou entidade que fabrica ou mantém o componente. Se o componente for livre e de código-fonte aberto, a correção de segurança deve ser partilhada de forma compatível com a licença desse componente, por exemplo, partilhando-a ao abrigo da mesma licença, ou de uma licença que permita ao responsável pela manutenção distribuir a correção ao abrigo da sua própria licença. Se o responsável pela manutenção desse componente dispuser de orientações sobre como partilhar as correções de segurança, o fabricante deve seguir essas orientações.

228. No entanto, o Regulamento de Ciber-Resiliência não obriga os fabricantes a garantir que as suas correções de segurança são necessariamente aceites pela pessoa ou entidade que fabrica ou mantém o componente. Também não são obrigados a assegurar que essas correções sejam necessariamente integradas no repositório de códigos do componente, por exemplo, quando o responsável pela manutenção preferir uma opção diferente para resolver o problema. Do mesmo modo, os fabricantes não são obrigados a aceitar uma correção proposta que o responsável pela manutenção do componente desenvolveu e podem preferir atenuar o problema de outras formas adequadas.

229. Em alguns casos, a pessoa ou entidade que fabrica ou mantém o componente pode já ter facultado uma correção de segurança para dar resposta à vulnerabilidade, mas um fabricante aplica uma estratégia de atenuação diferente (por exemplo, alterando uma configuração diferente). Nesses casos, o Regulamento de Ciber-Resiliência não exige que o fabricante partilhe a modificação de outra parte do sistema a montante. Todavia, incentiva-se o fabricante a fazê-lo sempre que tal possa apoiar a pessoa ou entidade que mantém o componente.

9.2.2. *Vulnerabilidades passíveis de serem exploradas conhecidas*

230. Um dos requisitos essenciais constantes da parte I do anexo I do Regulamento de Ciber-Resiliência prevê que, 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 ser disponibilizados no mercado sem nenhuma vulnerabilidade passível de ser explorada conhecida.

231. No artigo 3.º, ponto 41, define-se «vulnerabilidade passível de ser explorada» como «uma vulnerabilidade com potencial para ser efetivamente utilizada por um adversário em condições operacionais práticas». Nem todas as vulnerabilidades são passíveis de serem exploradas em condições operacionais práticas, e algumas vulnerabilidades só podem ser exploradas em condições teóricas (por exemplo, num laboratório ou numa simulação) e/ou não em condições que ocorreriam no ambiente operacional de um produto com elementos digitais.

232. O Regulamento de Ciber-Resiliência exige que os fabricantes disponham de políticas e procedimentos adequados para tratar e corrigir potenciais vulnerabilidades comunicadas a partir de fontes internas ou externas (artigo 13.º, n.º 8). Todavia, não indica explicitamente quando uma vulnerabilidade passível de ser explorada deve ser considerada do conhecimento do fabricante, desencadeando assim a obrigação de cumprir este requisito essencial no momento da colocação no mercado.

233. Uma vulnerabilidade deve ser considerada conhecida quando consta de bases de dados de vulnerabilidades pertinentes acessíveis ao público, como a base de dados europeia de vulnerabilidades criada pelo artigo 12.º, n.º 2, da Diretiva (UE) 2022/2555 ou outras bases de dados de vulnerabilidades proeminentes.

234. Além disso, uma vulnerabilidade também pode ser conhecida caso o fabricante tenha sido informado da mesma através de informações não públicas, por exemplo, da divulgação coordenada por um investigador no domínio da segurança ou dos seus próprios ensaios e análises internos, incluindo, por exemplo, ao utilizar serviços baseados na IA. Do mesmo modo, uma vulnerabilidade pode ser conhecida caso tenha sido divulgada publicamente e de forma proeminente em meios de comunicação social fiáveis, incluindo publicações especializadas em cibersegurança ou meios de comunicação social gerais.

235. No entanto, o simples facto de uma vulnerabilidade ser comunicada ou detetada não significa, por si só, que seja passível de ser explorada na prática ou aplicável ao produto com elementos digitais específico. O fabricante terá de a investigar e confirmar a veracidade dessas informações, bem como a aplicabilidade ao seu próprio produto com elementos digitais. Por conseguinte, pode decorrer um intervalo de tempo limitado entre o primeiro relatório da vulnerabilidade e a sua confirmação. Conforme indicado na secção *9.1 Obrigações em* matéria de comunicação de informações, a tónica deve ser colocada numa ação rápida para investigar e reagir.

236. Além disso, a obrigação de os fabricantes cumprirem os requisitos essenciais estabelecidos na parte I do anexo I aplica-se no momento da colocação no mercado, em conformidade com o artigo 13.º, n.º 1. Na prática, pode dar-se o caso de serem detetadas novas vulnerabilidades passíveis de serem exploradas durante as fases finais do ciclo de vida do desenvolvimento do produto com elementos digitais, incluindo pouco antes de entrar na cadeia de distribuição (e, por conseguinte, de ser colocado no mercado).

237. Uma vez que a obrigação de colocar no mercado produtos com elementos digitais sem vulnerabilidades conhecidas passíveis de serem exploradas é uma obrigação baseada no risco, cabe ao fabricante determinar se, com base na avaliação dos riscos de cibersegurança, o produto com elementos digitais pode ser colocado no mercado de forma segura, em conformidade com o Regulamento de Ciber-Resiliência. Em alternativa, o fabricante pode determinar que é necessário corrigir uma nova vulnerabilidade que possa ter chegado ao seu conhecimento antes de ser possível colocar o produto com elementos digitais no mercado. Ao proceder a essa determinação, os fabricantes deverão ter em conta a gravidade, a possibilidade de exploração e o potencial impacto da vulnerabilidade, bem como os riscos decorrentes para o próprio produto com elementos digitais quando for utilizado. Também podem ter em conta os riscos do adiamento do lançamento do produto até que a vulnerabilidade seja corrigida, por exemplo, porque o novo lançamento também dá resposta a outras vulnerabilidades passíveis de serem exploradas ou é necessário para a continuação do funcionamento de sistemas críticos. Em todo o caso, depois de um produto com elementos digitais ser colocado no mercado, o fabricante continua sujeito à obrigação de tratar as vulnerabilidades de forma eficaz e em conformidade com os requisitos de tratamento de vulnerabilidades estabelecidos na parte II do anexo I.

9.2.3. *Ensaios e análises eficazes e regulares*

238. A parte II, ponto 3, do anexo I exige que os fabricantes efetuem ensaios e análises eficazes e regulares do produto com elementos digitais ao longo do seu período de apoio. A realização de ensaios regulares não exige a repetição mecânica, a intervalos fixos, de uma campanha de ensaios inalterada. Significa analisar regularmente se as novas entradas de dados, como ameaças recentemente identificadas ou vulnerabilidades recentemente detetadas, exigem que os ensaios existentes sejam atualizados e executados em conformidade.

239. A frequência, o nível de pormenor e o conteúdo da análise devem ser proporcionados ao perfil de risco de cibersegurança do produto com elementos digitais, à sua evolução ao longo do tempo e ao estado do panorama das ameaças. Caso a análise identifique novas entradas de dados pertinentes que afetem o conjunto de ensaios, devem ser concebidos e executados ensaios novos ou modificados no produto, a fim de assegurar que nenhuma vulnerabilidade fica sem resposta. Tal pode incluir a repetição de ensaios existentes, caso uma modificação do produto com elementos digitais torne esses tipos de ensaios adequados, como os ensaios de regressão.

240. Se a análise não identificar tais entradas de dados, não é necessário conceber ensaios adicionais. Continuam a aplicar-se paralelamente outras obrigações de tratamento de vulnerabilidades, incluindo a de tratar e corrigir vulnerabilidades em relação aos riscos colocados.

9.3. **Interação com outros atos legislativos**

9.3.1. *Regulamento (UE) 2019/2144 e Regulamento (UE) n.º 168/2013*

241. O artigo 2.º, n.º 2, alínea c), do Regulamento de Ciber-Resiliência estabelece que o regulamento não é aplicável aos produtos com elementos digitais a que se aplica o Regulamento (UE) 2019/2144. O Regulamento (UE) 2019/2144 aplica-se aos «veículos das categorias M, N e O, tal como definidas no artigo 4.º do Regulamento (UE) 2018/858, e aos sistemas, componentes e unidades técnicas concebidos e construídos para esses veículos».

242. Do mesmo modo, o Regulamento Delegado (UE) 2025/1535 da Comissão excluiu os produtos com elementos digitais abrangidos pelo âmbito de aplicação do Regulamento (UE) n.º 168/2013 do âmbito de aplicação do Regulamento de Ciber-Resiliência. O Regulamento (UE) n.º 168/2013 aplica-se aos veículos da categoria L e «a sistemas, componentes e unidades técnicas, bem como [à]s peças e [a]o equipamento, concebidos e construídos para esses veículos» (artigo 2.º, n.º 1).

243. Os veículos a que esses regulamentos se aplicam não estão sujeitos ao Regulamento de Ciber-Resiliência. Além disso, são necessários esclarecimentos adicionais no que diz respeito ao âmbito de aplicação da isenção para sistemas, componentes, unidades técnicas separadas, peças e equipamentos (para efeitos da presente secção, «componentes») concebidos e construídos para tais veículos, que são considerados produtos com elementos digitais na aceção do Regulamento de Ciber-Resiliência.

244. Considera-se que esses componentes não estão sujeitos ao Regulamento de Ciber-Resiliência, desde que sejam exclusivamente concebidos e construídos para integração em veículos abrangidos pelos Regulamentos (UE) 2019/2144 e (UE) n.º 168/2013. Esta disposição aplica-se independentemente de o fabricante desse componente o vender diretamente ao fabricante do veículo ou a outro operador económico na cadeia de abastecimento do setor automóvel, desde que o componente seja claramente destinado e adequado apenas para integração final nesses veículos.

245. Em contrapartida, um fabricante que vende componentes genéricos que sejam produtos com elementos digitais passíveis de serem integrados em diferentes tipos de produtos, e não exclusivamente em veículos abrangidos por esses regulamentos, está sujeito ao Regulamento de Ciber-Resiliência.

246. A avaliação para determinar se um componente é colocado no mercado na aceção do Regulamento de Ciber--Resiliência deve basear-se nas condições objetivas em que é disponibilizado. Caso um fabricante ofereça um componente que não seja exclusivamente adequado para integração final nesses veículos através de canais de distribuição abertos a clientes fora da cadeia de abastecimento do setor automóvel, como pontos de venda a retalho gerais ou canais de venda em linha que aceitem encomendas do público em geral, esse componente é abrangido pelo âmbito de aplicação do Regulamento de Ciber-Resiliência, independentemente de quaisquer declarações relativas à sua utilização prevista. Nestas circunstâncias, não se pode considerar que o componente tenha sido concebido e construído exclusivamente para ser integrado em veículos abrangidos pelos Regulamentos (UE) 2019/2144 e (UE) n.º 168/2013, e o fabricante é obrigado a cumprir o disposto no Regulamento de Ciber--Resiliência. Em contrapartida, a utilização de canais restritos de distribuição empresa a empresa, limitados à cadeia de abastecimento do setor automóvel, pode indicar que é concebido e construído exclusivamente para essa integração.

9.3.2. *Validade dos certificados de exame UE de tipo (artigo 69.º, n.º 1)*

247. O artigo 69.º, n.º 1, do Regulamento de Ciber-Resiliência refere que «[o]s 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».

248. Deve entender-se que a manutenção da validade desses certificados e decisões de aprovação se limita aos riscos de cibersegurança e aos requisitos correspondentes abrangidos pela respetiva legislação de harmonização da União com base na qual foram emitidos. Para esses riscos, os fabricantes não são obrigados a reavaliar ou voltar a demonstrar a conformidade exclusivamente para efeitos do Regulamento de Ciber-Resiliência durante o período de validade referido no artigo 69.º, n.º 1, no caso de produtos com elementos digitais que tencionem colocar no mercado em 11 de dezembro de 2027, ou após essa data, e até 11 de junho de 2028 ([31]). Esta situação aplica-se aos certificados e às decisões de aprovação emitidos nos casos em que a legislação de harmonização da União aplicável exige que o fabricante realize o procedimento de avaliação da conformidade através de um organismo notificado, bem como nos casos em que o fabricante optou por fazê-lo voluntariamente.

249. Por conseguinte, a existência de um certificado ou de uma decisão de aprovação válidos ao abrigo de outra legislação de harmonização da União não isenta os fabricantes da realização de uma avaliação exaustiva dos riscos de cibersegurança ao abrigo do Regulamento de Ciber-Resiliência (nem de outras obrigações nele previstas). Em vez disso, permite-lhes recorrer às certificações existentes como prova de conformidade para o seu procedimento de avaliação da conformidade, na medida em que os riscos de cibersegurança correspondentes já estejam abrangidos. Caso o certificado ou a decisão de aprovação sejam válidos ao abrigo de outra legislação de harmonização da União que se prolongue para além de 11 de junho de 2028, o fabricante só pode, no entanto, recorrer a esse certificado ou decisão para efeitos do Regulamento de Ciber-Resiliência até 11 de junho de 2028.

250. Se a avaliação dos riscos de cibersegurança realizada em conformidade com o artigo 13.º, n.º 2, identificar riscos adicionais não abrangidos pelos requisitos de cibersegurança subjacentes ao certificado ou à decisão de aprovação existentes, os fabricantes continuam a ser responsáveis por dar resposta a esses riscos em conformidade com o Regulamento de Ciber-Resiliência. Nesses casos, o cumprimento exige que as lacunas identificadas sejam avaliadas e atenuadas, independentemente da manutenção da validade do certificado ou da decisão de aprovação existentes.

251. É possível ilustrar este cenário ao ter em conta o caso em que um produto com elementos digitais está sujeito aos requisitos de cibersegurança estabelecidos no Regulamento Delegado (UE) 2022/30 da Comissão que complementa a Diretiva 2014/53/UE [regulamento delegado da Diretiva Equipamento de Rádio (DER)] e em que foi emitido um certificado de exame UE de tipo ou uma decisão de aprovação com base nesses requisitos. Nesse caso, o certificado ou a decisão permanecem válidos, em conformidade com o artigo 69.º, n.º 1, no que se refere aos riscos de cibersegurança abrangidos por esse certificado e relacionados com os requisitos essenciais de cibersegurança constantes da Diretiva 2014/53/UE (Diretiva Equipamento de Rádio, ou «DER»).

252. Nesses casos, os fabricantes não são obrigados, para efeitos do Regulamento de Ciber-Resiliência, a reavaliar ou voltar a demonstrar a conformidade no que diz respeito aos riscos já tratados por esses certificados, enquanto o certificado ou a decisão de aprovação pertinentes permanecerem válidos e, em qualquer caso, não após 11 de junho de 2028. Tal inclui, por exemplo, riscos de cibersegurança relacionados com a proteção da rede, a proteção de dados pessoais e da privacidade ou a prevenção de fraudes (na medida em que esses riscos estejam abrangidos por esse certificado) relacionados com os requisitos de cibersegurança constantes da DER e refletidos na avaliação da conformidade.

253. Todavia, se a avaliação dos riscos de cibersegurança realizada em conformidade com o artigo 13.º, n.º 2, do Regulamento de Ciber-Resiliência identificar riscos de cibersegurança adicionais não abrangidos por esses certificados, os fabricantes continuam a ser responsáveis por dar resposta a esses riscos em conformidade com o Regulamento de Ciber-Resiliência. Tal pode incluir, por exemplo, riscos relacionados com os processos de tratamento de vulnerabilidades, a minimização dos dados e a redução da superfície de ataque, ou outros aspetos de cibersegurança específicos do produto não tratados por esses certificados ou, em qualquer caso, não abrangidos pelos requisitos essenciais de cibersegurança constantes da DER.

254. Por conseguinte, a existência de um certificado de exame UE de tipo ou de uma decisão de aprovação válidos ao abrigo da DER para os seus requisitos essenciais em matéria de cibersegurança não demonstra, por si só, a plena conformidade com o Regulamento de Ciber-Resiliência. Em vez disso, permite que os fabricantes recorram a esse certificado ou a essa decisão como prova de conformidade para os riscos correspondentes, assegurando simultaneamente que quaisquer riscos remanescentes ou recentemente identificados sejam avaliados e atenuados em conformidade com o Regulamento de Ciber-Resiliência.

([31]) Os produtos com elementos digitais colocados no mercado antes de 11 de dezembro de 2027 estão sujeitos à legislação da União aplicável no momento da sua colocação no mercado e, se estiverem em conformidade, podem ser vendidos e colocados em funcionamento, a menos que sejam, em 11 de dezembro de 2027 ou após essa data, objeto de modificações substanciais. Para os conceitos de «colocação no mercado» e «disponibilização no mercado», ver também a secção *2.1 Colocação no mercado* do presente documento, bem como o capítulo 2 do Guia Azul.

255. Do mesmo modo, se um produto com elementos digitais estiver sujeito aos requisitos essenciais de saúde e segurança relacionados com a cibersegurança estabelecidos no Regulamento (UE) 2023/1230 (Regulamento Máquinas), plenamente aplicável a partir de 20 de janeiro de 2027, e se tiver sido emitido um certificado de exame UE de tipo ou uma decisão de aprovação com base nesses requisitos, esse certificado ou essa decisão de aprovação permanece válido, em conformidade com o artigo 69.º, n.º 1, do Regulamento de Ciber-Resiliência, no que se refere aos riscos de cibersegurança abrangidos pelo Regulamento Máquinas.

256. Trata-se, em especial, de aspetos de cibersegurança relacionados com a proteção contra a corrupção e com a segurança e fiabilidade dos sistemas de comando, conforme estabelecido as secções 1.1.9 e 1.2.1 do anexo III do Regulamento Máquinas. Para esses riscos, os fabricantes não são obrigados, para efeitos do Regulamento de Ciber--Resiliência, a reavaliar ou a voltar a demonstrar a conformidade enquanto o certificado ou a decisão de aprovação pertinentes permanecerem válidos e, em qualquer caso, não após 11 de junho de 2028. Esta disposição aplica-se na medida em que esses riscos tenham sido tratados no âmbito da avaliação da conformidade ao abrigo do Regulamento Máquinas.

257. Como acontece com os requisitos essenciais de cibersegurança constantes da DER referidos *supra*, caso a avaliação dos riscos de cibersegurança realizada nos termos do artigo 13.º, n.º 2, do Regulamento de Ciber-Resiliência identifique riscos de cibersegurança adicionais não abrangidos pelo certificado pertinente emitido nos termos do Regulamento Máquinas e que estejam relacionados com os requisitos de cibersegurança constantes desse regulamento, os fabricantes continuam a ser responsáveis por fazer face a esses riscos em conformidade com o Regulamento de Ciber-Resiliência.