Jornal Oficial
da União Europeia

PT
Série L

2025/2392

1.12.2025

REGULAMENTO DE EXECUÇÃO (UE) 2025/2392 DA COMISSÃO

de 28 de novembro de 2025

relativo à descrição técnica das categorias de produtos importantes e críticos com elementos digitais nos termos do Regulamento (UE) 2024/2847 do Parlamento Europeu e do Conselho

(Texto relevante para efeitos do EEE)

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta 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]), nomeadamente o artigo 7.º, n.º 4,

Considerando o seguinte:

(1) O Regulamento (UE) 2024/2847 estabelece regras relativas à cibersegurança dos produtos com elementos digitais. Em especial, o anexo III desse regulamento estabelece categorias de produtos importantes com elementos digitais que, quando colocados no mercado, estão sujeitos a procedimentos de avaliação da conformidade mais rigorosos do que os aplicáveis a outros produtos com elementos digitais. O anexo IV do Regulamento (UE) 2024/2847 estabelece as categorias de produtos críticos com elementos digitais para as quais os fabricantes podem ser obrigados a obter um certificado europeu de cibersegurança ao abrigo de um sistema europeu de certificação da cibersegurança nos termos do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho ([2]) ou que estarão sujeitos a uma avaliação da conformidade por terceiros obrigatória, quando colocados no mercado.

(2) Nos termos do artigo 7.º, n.º 1, e do artigo 8.º, n.º 1, do Regulamento (UE) 2024/2847, a funcionalidade principal de um produto com elementos digitais determina se esse produto se enquadra na descrição técnica de categoria de produtos importantes ou críticos com elementos digitais e, por conseguinte, está sujeito aos procedimentos de avaliação da conformidade aplicáveis.

(3) Ao desenvolverem um produto com elementos digitais, e a fim de alcançar o conjunto de funcionalidades desejado, os fabricantes integram normalmente nos seus próprios produtos com elementos digitais outros componentes que são também produtos com elementos digitais e que podem corresponder à descrição técnica de categoria de produtos importantes ou críticos. Nos termos do Regulamento (UE) 2024/2847, um produto com elementos digitais está sujeito aos procedimentos de avaliação da conformidade aplicáveis a produtos importantes ou críticos com elementos digitais, se esse produto no seu conjunto for um produto importante ou crítico, tal como estabelecido nos anexos III e IV desse regulamento. Por exemplo, a integração de um navegador incorporado como componente de uma aplicação de notícias para utilização em telemóveis inteligentes não sujeita, por si só, a aplicação de notícias ao procedimento de avaliação da conformidade aplicável aos produtos com elementos digitais que têm a funcionalidade principal de «navegadores autónomos e incorporados». No entanto, em conformidade com o Regulamento (UE) 2024/2847, o fabricante deve assegurar que o produto com elementos digitais no seu conjunto cumpre os requisitos essenciais de cibersegurança. Por conseguinte, tem de avaliar a segurança de todo o produto, tendo em conta, conforme adequado, a segurança dos componentes ou as funcionalidades nele integrados. Por exemplo, para que o fabricante de uma aplicação de notícias demonstre que o seu produto com elementos digitais está em conformidade com o Regulamento (UE) 2024/2847, deve demonstrar que a aplicação no seu conjunto cumpre os requisitos aplicáveis, tendo em conta, conforme adequado, a segurança do navegador incorporado que está integrado na aplicação.

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

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

(4) O facto de um produto com elementos digitais desempenhar funções diferentes ou adicionais às indicadas nas descrições técnicas estabelecidas neste regulamento não significa, por si só, que o produto com elementos digitais não tem a funcionalidade principal de uma categoria de produtos constante dos anexos III e IV do Regulamento (UE) 2024/2847. Por exemplo, os produtos com elementos digitais que têm a funcionalidade principal de «sistemas operativos» incluem frequentemente *software* que desempenha funções auxiliares não incluídas na descrição técnica dessa categoria de produtos, como calculadoras ou programas simples de edição gráfica. Os produtos com elementos digitais também incorporam muitas vezes componentes que têm a funcionalidade de outro produto importante ou crítico com elementos digitais, como é o caso de um sistema operativo que integre uma funcionalidade de navegador ou de um encaminhador que integre uma funcionalidade de barreira de segurança (*firewall*). No entanto, tal não significa, por si só, que esses produtos com elementos digitais não tenham a funcionalidade principal de «sistemas operativos» ou «encaminhadores, *modems* para ligação à Internet e comutadores», respetivamente.

(5) Por outro lado, não se deve considerar que um produto com elementos digitais que tenha capacidade para desempenhar as funções de uma categoria de produtos estabelecida nos anexos III e IV do Regulamento (UE) 2024/2847, mas cuja funcionalidade principal seja diferente da funcionalidade dessa categoria de produtos, corresponde à descrição técnica dessa categoria. Por exemplo, 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, analisá-los e apresentá-los como informações práticas para fins de segurança. No entanto, uma vez que a sua funcionalidade principal não é a de um SIEM, não se deve, de modo geral, considerar que o *software* de OARS corresponde à descrição técnica dos «sistemas de gestão de informações e eventos de segurança (SIEM)». Do mesmo modo, um telemóvel inteligente integra normalmente componentes que desempenham as funções de várias categorias de produtos estabelecidas nos anexos III e IV do Regulamento (UE) 2024/2847, como um sistema operativo ou um gestor de senhas integrado. No entanto, uma vez que a funcionalidade principal de um telemóvel inteligente não é a de um sistema operativo ou a de um gestor de senhas, não se deve geralmente considerar que corresponde à descrição técnica dessas categorias de produtos.

(6) Nos termos do artigo 13.º, n.ºs 2 e 3, do Regulamento (UE) 2024/2847, os fabricantes de produtos com elementos digitais devem aplicar os requisitos essenciais de cibersegurança constantes da parte I do anexo I do Regulamento (UE) 2024/2847 de forma proporcional aos riscos do produto com elementos digitais, com base na finalidade prevista, na utilização razoavelmente previsível e nas condições de utilização do produto com elementos digitais, tendo em conta o período de tempo estimado de utilização do produto. Em conformidade com o artigo 13.º, n.ºs 2 e 3, do referido regulamento, e independentemente de o produto com elementos digitais ser considerado um produto importante ou crítico com elementos digitais, os fabricantes devem realizar uma avaliação exaustiva dos riscos de cibersegurança e indicar a forma como os requisitos essenciais de cibersegurança são aplicados com base na avaliação dos riscos, incluindo os seus ensaios e garantias. Se a funcionalidade principal do seu produto com elementos digitais corresponder à descrição técnica de um produto importante ou crítico com elementos digitais, os fabricantes devem demonstrar a conformidade de acordo com os procedimentos específicos de avaliação da conformidade estabelecidos no artigo 32.º, n.ºs 2, 3, 4 e 5 do Regulamento (UE) 2024/2847.

(7) Este regulamento inclui exemplos de produtos com elementos digitais cuja funcionalidade principal corresponde à descrição técnica de determinados produtos importantes ou críticos com elementos digitais. Estes exemplos são apresentados apenas para efeitos ilustrativos e não constituem uma lista exaustiva.

(8) Para proporcionar segurança jurídica aos fabricantes, as categorias de produtos com elementos digitais que são microprocessadores invioláveis, microcontroladores invioláveis, cartões inteligentes ou dispositivos semelhantes, incluindo elementos seguros, devem ser distinguidos com base no nível de resistência à potencial exploração de falhas ou pontos fracos para o qual foram concebidos. O nível AVA_VAN é uma forma extensivamente utilizada e normalizada para expressar esse nível de resistência. Os níveis AVA_VAN estão estabelecidos nas normas dos Critérios Comuns e da Metodologia Comum de Avaliação disponíveis ao público, em que se basearam os quadros de certificação existentes amplamente adotados no mercado, como o Regulamento de Execução (UE) 2024/482 da

Comissão ([3]), que estabelece um sistema europeu de certificação da cibersegurança que pode ser utilizado para certificar um produto a um nível específico de garantia. Baseado em práticas mundiais, este regulamento de execução prevê a possibilidade de emitir certificados a partir de versões mais antigas das normas até ao final de 2027. Por conseguinte, no contexto do Regulamento (UE) 2024/2847, é adequado permitir que os níveis AVA_VAN sejam expressos por referência à versão mais recente ou a versões mais antigas dessas normas.

(9) As medidas previstas no presente regulamento estão em conformidade com o parecer do Comité instituído pelo artigo 62.º, n.º 1, do Regulamento (UE) 2024/2847,

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

Definições

Para efeitos do presente regulamento, entende-se por:

1) «Critérios Comuns», os Critérios Comuns para a Avaliação da Segurança das Tecnologias da Informação, tal como definidos no artigo 2.º, n.º 1, do Regulamento de Execução (UE) 2024/482 ou estabelecidos nas normas referidas no artigo 3.º, n.º 2, alíneas a) e b), desse regulamento de execução;

2) «Metodologia Comum de Avaliação», a Metodologia Comum para a Avaliação da Segurança das Tecnologias da Informação, tal como definida no artigo 2.º, n.º 2, do Regulamento de Execução (UE) 2024/482 ou estabelecida nas normas referidas no artigo 3.º, n.º 2, alíneas c) e d), desse regulamento de execução.

Artigo 2.º

1. A descrição técnica das categorias de produtos com elementos digitais das classes I e II enumeradas no anexo III do Regulamento (UE) 2024/2847 é estabelecida no anexo I do presente regulamento.

2. A descrição técnica das categorias de produtos com elementos digitais enumeradas no anexo IV do Regulamento (UE) 2024/2847 é estabelecida no anexo II do presente regulamento.

Artigo 3.º

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

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

Feito em Bruxelas, em 28 de novembro de 2025.

Pela Comissão
A Presidente
Ursula VON DER LEYEN

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

ANEXO I

PRODUTOS IMPORTANTES COM ELEMENTOS DIGITAIS

Classe I

Categoria de produtos	Descrição técnica
1. Sistemas de gestão de identidade e *software* e *hardware* de gestão de acesso privilegiado, nomeadamente leitores de autenticação e controlo do acesso, incluindo leitores biométricos	Os sistemas de gestão de identidade são produtos com elementos digitais que disponibilizam mecanismos de autenticação ou autorização e que podem também disponibilizar mecanismos para a gestão do ciclo de vida das credenciais de identidade de pessoas singulares, pessoas coletivas, dispositivos ou sistemas, como o registo, a disponibilização, a manutenção e o cancelamento do registo de identidade. Estes sistemas incluem sistemas de gestão de acesso que controlam o acesso de pessoas singulares, pessoas coletivas, dispositivos ou sistemas a recursos digitais ou a locais físicos. O *software* de gestão de acesso privilegiado é um sistema de gestão de acesso que controla e monitoriza os direitos de acesso a sistemas de tecnologia informática ou operacional e a informações sensíveis dentro de uma organização, incluindo sistemas que aplicam políticas diferenciadas de controlo do acesso para utilizadores privilegiados. Esta categoria inclui, entre outros, os leitores de autenticação e controlo de acesso, os leitores biométricos, o *software* de autenticação única, o *software* de gestão de identidade federado, o *software* de senha de utilização única, os dispositivos de autenticação de *hardware*, como geradores de códigos de autorização da transação, o *software* de autenticação e o *software* de autenticação multifatores.
2. Navegadores autónomos e incorporados	Produtos de *software* com elementos digitais que permitem aos utilizadores finais aceder, transmitir e interagir com conteúdos e serviços Web alojados em servidores ligados a redes como a Internet. Normalmente, incluem um motor de navegação para interpretação e visualização de conteúdos escritos em linguagem de marcação (por exemplo, HTML), apoio a protocolos Web (por exemplo, HTTP, HTTPS), a capacidade de executar *scripts* e gerir as entradas dos utilizadores, bem como o armazenamento de dados temporários ou persistentes de sítios Web (testemunhos de conexão). Esta categoria inclui, entre outros, as aplicações autónomas que desempenham as funções de navegadores, os navegadores incorporados destinados à integração noutro sistema ou aplicação, bem como os navegadores com integração de agentes de IA.
3. Gestores de senhas	Produtos com elementos digitais que armazenam senhas, localmente num dispositivo ou num servidor remoto, incluindo atividades como a geração de senhas, a partilha de senhas e a integração com aplicações locais ou de terceiros para a utilização de senhas. Esta categoria inclui, entre outros, os gestores de senhas locais, os gestores de senhas disponibilizados como extensões do navegador, os gestores de senhas empresariais, bem como os gestores de senhas baseados em *hardware*.

Categoria de produtos	Descrição técnica
4. *Software* de pesquisa, remoção ou colocação em quarentena de *software* malicioso	Produtos de *software* com elementos digitais, geralmente designados por antivírus ou *antimalware*, que detetam ou pesquisam *software* ou código malicioso em dispositivos, ou que removem ou colocam em quarentena esse *software* ou código para manter a integridade, a confidencialidade ou a disponibilidade desses dispositivos. No contexto desta categoria de produtos, entende-se por *software* malicioso aquele que contém funcionalidades ou capacidades mal-intencionadas que podem causar danos, direta ou indiretamente, ao utilizador e/ou ao sistema informático, tais como vírus, vermes, *software* de sequestro, *software* espião e cavalos de Troia. Esta categoria inclui, entre outros, o *software* que deteta ou pesquisa *software* malicioso em tempo real ou manualmente, *software* de deteção de dissimuladores de atividade e discos de recuperação com a funcionalidade central de pesquisa, remoção ou colocação em quarentena de *software* malicioso.
5. Produtos com elementos digitais com a função de rede privada virtual (VPN)	Produtos com elementos digitais que estabelecem um túnel lógico encriptado, criado a partir dos recursos do sistema de uma rede física ou virtual. Esta categoria inclui, entre outros, os clientes de redes privadas virtuais, os servidores de redes privadas virtuais e os pontos de acesso às redes privadas virtuais.
6. Sistemas de gestão de rede	Produtos com elementos digitais que gerem elementos de rede conectados, como servidores, encaminhadores, comutadores, estações de trabalho, impressoras ou dispositivos móveis, monitorizando-os e controlando a sua configuração e operações de rede. Esta categoria inclui, entre outros, os sistemas de gestão de ponta a ponta e os sistemas específicos de gestão de configuração, como os controladores para a ligação em rede definida por *software*.
7. Sistemas de gestão de informações e eventos de segurança (SIEM)	Produtos com elementos digitais que recolhem dados de várias fontes, analisam e correlacionam esses dados e os apresentam como informações práticas para fins relacionados com a cibersegurança, como a deteção de ameaças e incidentes, a análise forense ou a conformidade.
8. Gestores de arranque	Produtos de *software* com elementos digitais que gerem o processo de arranque inicial do sistema após a ligação/ /reinício, iniciando o *hardware*, carregando ou transferindo o controlo para o ambiente do sistema operativo ou para os recursos do sistema e selecionando opções de arranque. Esta categoria inclui, entre outros, o *firmware* UEFI e os carregadores de arranque de uma e de várias fases.
9. Infraestruturas de chaves públicas e *software* de emissão de certificados digitais	Produtos com elementos digitais utilizados como parte de uma infraestrutura de chaves públicas (ICP) que gerem a validação, criação, emissão, distribuição, publicação do estado, renovação ou revogação de certificados digitais, ou a geração, armazenamento, caução, troca, destruição ou rotação de chaves criptográficas associadas a esses certificados digitais. Esta categoria inclui, entre outros, os sistemas de gestão de chaves, os sistemas de gestão de certificados digitais, os respondedores do protocolo de estado dos certificados em linha e as soluções ICP multifuncionais.

Categoria de produtos	Descrição técnica
10. Interfaces físicas e virtuais da rede	As interfaces físicas da rede são produtos com elementos digitais que ligam diretamente um dispositivo a uma rede através de uma interface de programação de aplicações (IPA) fornecida pelos controladores da interface, operando normalmente na camada de ligação de dados, e que incluem adaptadores de *hardware* para os meios de transmissão com *firmware* correspondente, operando normalmente na camada física e de ligação de dados. As interfaces virtuais da rede são produtos com elementos digitais que ligam direta ou indiretamente um dispositivo a uma rede através de uma IPA que emula a dos controladores de interfaces físicas da rede, operando normalmente na camada de ligação de dados. Esta categoria inclui, entre outros, as placas de rede com e sem fios, os controladores e adaptadores nomeadamente para Wi-Fi, Ethernet, IrDA, USB, Bluetooth, NearLink, Zigbee ou Fieldbus, bem como os produtos autónomos puramente virtuais, como as placas de rede virtuais, as interfaces de rede de contentores e as interfaces de VPN.
11. Sistemas operativos	Produtos de *software* com elementos digitais que fornecem uma interface abstrata do *hardware* subjacente e controlam a execução do *software*, podendo prestar serviços como a gestão e a configuração dos recursos informáticos, a programação, o controlo de entrada/saída, a gestão de dados e a disponibilização de uma interface através da qual as aplicações interagem com os periféricos e os recursos do sistema. Esta categoria inclui, entre outros, os sistemas operativos em tempo real, os sistemas operativos de aplicação geral e os sistemas operativos de aplicação específica.
12. Encaminhadores, *modems* para ligação à Internet e comutadores	Os encaminhadores são produtos com elementos digitais que estabelecem e controlam o fluxo de dados entre diferentes redes, através da seleção de vias ou itinerários com mecanismos e algoritmos de protocolo de encaminhamento, operando normalmente na camada de rede. Esta categoria inclui, entre outros, os encaminhadores com e sem fios, os encaminhadores virtuais e os encaminhadores com ou sem *modems*.
	Os *modems* destinados à ligação à Internet são produtos de *hardware* com elementos digitais que utilizam técnicas de modulação e desmodulação digitais para converter sinais analógicos de e para sinais digitais para comunicações baseadas no IP. Esta categoria inclui, entre outros, os *modems* de fibra ótica, os *modems* de linha de assinante digital (DSL), os *modems* de cabo (DOCSIS), os *modems* de satélite e os *modems* celulares.
	Os comutadores são produtos com elementos digitais que asseguram a conectividade entre os dispositivos ligados em rede através de mecanismos de encaminhamento de pacotes e que possuem um plano de gestão, implementado normalmente na camada de ligação de dados ou de rede. Esta categoria inclui, entre outros, os comutadores geridos, os comutadores inteligentes, os comutadores multicamadas, os comutadores de segurança virtual, os comutadores programáveis para redes definidas por *software* e as pontes, como os pontos de acesso sem fios.

Categoria de produtos	Descrição técnica
13. Microprocessadores com funcionalidades relacionadas com a cibersegurança	Produtos com elementos digitais que são circuitos integrados e que desempenham funções de processamento central assentes em memória externa e periféricos, incluindo microcódigo e outro *firmware* de baixo nível. Além disso, proporcionam funcionalidades relacionadas com a cibersegurança, como a encriptação, a autenticação, o armazenamento seguro de chaves, a geração de números aleatórios, o ambiente de execução de confiança ou outros mecanismos de proteção baseados em *hardware* que visam proteger outros produtos, redes ou serviços para além do próprio microprocessador, como a cadeia de arranque seguro, a virtualização ou as interfaces de comunicação seguras.
14. Microcontroladores com funcionalidades relacionadas com a cibersegurança	Produtos com elementos digitais que são circuitos integrados que desempenham funções de processamento central com memória integrada que permite que o microcontrolador seja programável e, normalmente, também outros periféricos, como o microcódigo e outro *firmware* de baixo nível. Além disso, proporcionam funcionalidades relacionadas com a cibersegurança, como a encriptação, a autenticação, o armazenamento seguro de chaves, a geração de números aleatórios, o ambiente de execução de confiança ou outros mecanismos de proteção baseados em *hardware* que visam proteger outros produtos, redes ou serviços para além do próprio microcontrolador, como a cadeia de arranque seguro, a virtualização ou as interfaces de comunicação seguras.
15. Circuitos integrados de aplicação específica (ASIC) e redes de portas lógicas programáveis (FPGA) com funcionalidades relacionadas com a cibersegurança	Os circuitos integrados de aplicação específica (ASIC) com funcionalidades relacionadas com a cibersegurança são produtos com elementos digitais que são circuitos integrados, total ou parcialmente personalizados para desempenhar uma função específica ou implementar uma aplicação específica, incluindo microcódigo e outro *firmware* de baixo nível. Além disso, proporcionam funcionalidades relacionadas com a cibersegurança, como a encriptação, a autenticação, o armazenamento seguro de chaves, a geração de números aleatórios, o ambiente de execução de confiança ou outros mecanismos de proteção baseados em *hardware* que visam proteger outros produtos, redes ou serviços para além dos próprios ASIC, como a cadeia de arranque seguro, a virtualização ou as interfaces de comunicação seguras.
	As redes de portas lógicas programáveis (FPGA) com funcionalidades relacionadas com a cibersegurança são produtos com elementos digitais que são circuitos integrados caracterizados por uma matriz de blocos lógicos configuráveis concebidos para serem reprogramáveis após o fabrico para executar uma função específica ou implementar uma aplicação específica, incluindo microcódigo e outro *firmware* de baixo nível. Além disso, proporcionam funcionalidades relacionadas com a cibersegurança, como a encriptação, a autenticação, o armazenamento seguro de chaves, a geração de números aleatórios, o ambiente de execução de confiança ou outros mecanismos de proteção baseados em *hardware* que visam proteger outros produtos, redes ou serviços para além das próprias FPGA, como a cadeia de arranque seguro, a virtualização ou as interfaces de comunicação seguras.
16. Assistentes virtuais de uso geral para residências inteligentes	Produtos com elementos digitais que comunicam na Internet pública, diretamente ou através de outros equipamentos, que processam tarefas, perguntas ou pedidos baseados em instruções de linguagem natural, como entradas em formato áudio ou escrito, e que, com base nessas tarefas, perguntas ou pedidos, proporcionam acesso a outros serviços ou controlam as funções de dispositivos conectados em contextos residenciais. Esta categoria inclui, entre outros, as colunas inteligentes com um assistente virtual integrado e os assistentes virtuais autónomos que correspondam a esta descrição.

Categoria de produtos	Descrição técnica
17. Produtos domésticos inteligentes com funcionalidades de segurança, incluindo fechaduras inteligentes, câmaras de segurança, sistemas de monitorização de bebés e sistemas de alarme	Produtos com elementos digitais que protegem a segurança física dos consumidores num contexto residencial e que podem ser controlados ou geridos remotamente a partir de outros sistemas, bem como *hardware* e *software* capazes de controlar centralmente esses produtos. Esta categoria inclui, entre outros, os dispositivos inteligentes de fecho de portas, os sistemas de monitorização de bebés, os sistemas de alarme e as câmaras de segurança residencial.
18. Brinquedos ligados à Internet, abrangidos pela Diretiva 2009/48/CE do Parlamento Europeu e do Conselho ([1]), com características sociais interativas (por exemplo, que falam ou filmam) ou que têm características de localização	Os brinquedos ligados à Internet com características sociais interativas são produtos com elementos digitais abrangidos pela Diretiva 2009/48/CE, que comunicam na Internet pública, diretamente ou através de qualquer outro equipamento, e que dispõem de tecnologias incorporadas que permitem a comunicação de entrada e saída, como teclados, microfones, colunas ou câmaras.
	Os brinquedos ligados à Internet com características de localização são produtos com elementos digitais abrangidos pela Diretiva 2009/48/CE, que comunicam na Internet pública, diretamente ou através de qualquer outro equipamento, e que dispõem de tecnologias que permitem rastrear ou inferir a localização geográfica do brinquedo ou do seu utilizador. Quando o brinquedo se limita a detetar a proximidade do utilizador ou de outros brinquedos utilizando tecnologias de deteção, considera-se que o brinquedo não tem características de localização.
19. Produtos pessoais usáveis, para usar ou colocar no corpo humano, destinados à monitorização do estado de saúde (p. ex., rastreio) e aos quais não se aplicam o Regulamento (UE) 2017/745 ([2]) ou (UE) 2017/746 ([3]) do Parlamento Europeu e do Conselho, ou produtos pessoais usáveis, a utilizar por crianças ou a estas destinados	Os produtos pessoais usáveis, para usar ou colocar no corpo humano, destinados à monitorização do estado de saúde são produtos com elementos digitais usados diretamente no corpo ou através de vestuário ou acessórios e que podem, de forma regular ou contínua, detetar e processar informações, incluindo métricas corporais pertinentes para a saúde do utilizador, excluindo os produtos abrangidos pelo âmbito de aplicação do Regulamento (UE) 2017/745 ou do Regulamento (UE) 2017/746. Esta categoria inclui, entre outros, os monitores de atividade física, os relógios inteligentes, os adornos inteligentes, o vestuário inteligente e o equipamento desportivo que correspondam a esta descrição.
	Os produtos pessoais usáveis, a utilizar por crianças ou a estas destinados são produtos com elementos digitais que podem ser usados ou colocados no corpo, diretamente ou através de vestuário ou acessórios, de pessoas com menos de 14 anos. Esta categoria inclui, entre outros, os dispositivos de segurança usáveis para crianças.

([1]) Diretiva 2009/48/CE do Parlamento Europeu e do Conselho, de 18 de junho de 2009, relativa à segurança dos brinquedos (JO L 170 de 30.6.2009, p. 1, ELI: http://data.europa.eu/eli/dir/2009/48/oj).

([2]) Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho, de 5 de abril de 2017, relativo aos dispositivos médicos, que altera a Diretiva 2001/83/CE, o Regulamento (CE) n.º 178/2002 e o Regulamento (CE) n.º 1223/2009 e que revoga as Diretivas 90/385/CEE e 93/42/CEE do Conselho (JO L 117 de 5.5.2017, p. 1, ELI: http://data.europa.eu/eli/reg/2017/745/oj).

([3]) Regulamento (UE) 2017/746 do Parlamento Europeu e do Conselho, de 5 de abril de 2017, relativo aos dispositivos médicos para diagnóstico *in vitro* e que revoga a Diretiva 98/79/CE e a Decisão 2010/227/UE da Comissão (JO L 117 de 5.5.2017, p. 176, ELI: http://data.europa.eu/eli/reg/2017/746/oj).

Classe II

Categoria de produtos	Descrição técnica
1. Hipervisores e sistemas *container runtime* que permitam a execução virtualizada de sistemas operativos e ambientes semelhantes	Os hipervisores são produtos de *software* com elementos digitais que asseguram a abstração e/ou a atribuição de recursos informáticos e permitem a execução, gestão e orquestração de máquinas virtuais que estão logicamente separadas entre si e/ou do *hardware* físico. Os hipervisores podem funcionar diretamente em *hardware* (*bare metal*), em complemento de um sistema operativo, ou no interior de outra máquina virtual (virtualização aninhada). No contexto desta categoria de produtos, uma máquina virtual é uma separação lógica definida pelo *software* de um ambiente informático, que inclui um conjunto virtualizado de recursos de *hardware* (por exemplo, CPU, memória, armazenamento, interfaces de rede) e geralmente aloja o seu próprio sistema operativo. Esta categoria inclui, entre outros, os hipervisores de tipo 1 (*bare metal*), os hipervisores de tipo 2 (alojados num sistema operativo) e os hipervisores híbridos.
	Os sistemas *container runtime* são produtos de *software* com elementos digitais que gerem a execução e o ciclo de vida dos contentores que funcionam num único sistema operativo anfitrião enquanto processos isolados, atribuindo recursos e permitindo a gestão e a orquestração de contentores individuais. No contexto desta categoria de produtos, um contentor é um ambiente de execução baseado em *software* que encerra um ou mais componentes de *software* e as suas dependências num único pacote, permitindo-lhe funcionar de forma independente e coerente.
2. Barreiras de segurança, sistemas de deteção e prevenção de intrusões	As barreiras de segurança são produtos com elementos digitais que protegem um sistema ou rede conectados contra o acesso não autorizado através da monitorização e restrição do tráfego de comunicações de dados de e para essa rede. Esta categoria inclui, entre outros, as barreiras de segurança da rede e as barreiras de segurança das aplicações, como filtros ou barreiras de segurança de aplicações Web e os pontos de acesso contra o correio eletrónico não solicitado.
	Os sistemas de deteção de intrusões são produtos com elementos digitais que monitorizam o tráfego assim que entra no ambiente de rede para localizar atividades suspeitas e detetam ou identificam que foi tentada, está a ocorrer ou já ocorreu uma intrusão num sistema ou rede conectados. Esta categoria inclui, entre outros, os sistemas de deteção de intrusões baseados na rede e os sistemas de deteção de intrusões baseados no anfitrião.
	Os sistemas de prevenção de intrusões são produtos com elementos digitais compostos por um sistema de deteção de intrusões que responde ativamente a uma intrusão num sistema ou rede conectados. Esta categoria inclui, entre outros, os sistemas de prevenção de intrusões baseados na rede e os sistemas de prevenção de intrusões baseados no anfitrião.

Categoria de produtos	Descrição técnica
3. Microprocessadores invioláveis	Produtos com elementos digitais que sejam microprocessadores com funcionalidades relacionadas com a cibersegurança referidos no quadro «Classe I», ponto 13, do presente anexo, incluindo provas de manipulação, resistência ou resposta, e que, adicionalmente, sejam concebidos para proporcionar proteção de nível AVA_VAN 2 ou 3, tal como estabelecido nos Critérios Comuns e na Metodologia Comum de Avaliação.
4. Microcontroladores invioláveis	Produtos com elementos digitais que sejam microprocessadores com funcionalidades relacionadas com a cibersegurança referidos no quadro «Classe I», ponto 14, do presente anexo, incluindo provas de manipulação, resistência ou resposta, e que, adicionalmente, sejam concebidos para proporcionar proteção de nível AVA_VAN 2 ou 3, tal como estabelecido nos Critérios Comuns e na Metodologia Comum de Avaliação.

ELI: http://data.europa.eu/eli/reg_impl/2025/2392/oj

ANEXO II

PRODUTOS CRÍTICOS COM ELEMENTOS DIGITAIS

Categoria de produtos	Descrição técnica
1. Dispositivos de *hardware* com caixas de segurança	Produtos de *hardware* com elementos digitais que armazenam, processam ou gerem, de forma segura, dados sensíveis ou realizam operações criptográficas, sendo compostos por múltiplos componentes discretos, incorporando um invólucro físico de *hardware* que fornece provas de manipulação, resistência ou resposta como contramedidas contra ataques físicos. Esta categoria inclui, entre outros, os terminais físicos de pagamento, os módulos de segurança de *hardware* que geram e gerem elementos criptográficos e tacógrafos que correspondam à descrição acima.
2. Pontos de acesso para contadores inteligentes no âmbito de sistemas de contadores inteligentes, conforme definidos no artigo 2.º, ponto 23, da Diretiva (UE) 2019/944 do Parlamento Europeu e do Conselho ([1]), e outros dispositivos para fins avançados de segurança, incluindo o criptoprocessamento seguro	Os pontos de acesso para contadores inteligentes são produtos com elementos digitais que controlam a comunicação entre componentes integrados ou ligados a sistemas de contadores inteligentes, na aceção do artigo 2.º, n.º 23, da Diretiva (UE) 2019/944, e terceiros autorizados, como prestadores de serviços públicos. Os pontos de acesso para contadores inteligentes recolhem, processam e armazenam dados do contador ou dados pessoais, protegem os fluxos de dados e informações através do apoio a necessidades criptográficas específicas, como a encriptação e a desencriptação de dados, incorporam funcionalidades de barreira de segurança e proporcionam os meios para controlar outros dispositivos. Esta categoria inclui, entre outros, os pontos de acesso para contadores inteligentes associados a sistemas de contadores inteligentes que medem a eletricidade, na aceção do artigo 2.º, n.º 23, da Diretiva (UE) 2019/944. Pode também incluir pontos de acesso para contadores inteligentes utilizados noutros sistemas de contadores inteligentes que meçam o consumo de outras fontes de energia como o gás ou o calor, desde que o ponto de acesso corresponda a esta descrição.
3. Cartões inteligentes ou dispositivos semelhantes, incluindo elementos seguros	Os elementos seguros são microcontroladores ou microprocessadores com funcionalidades relacionadas com a cibersegurança e que incluem provas de manipulação, resistência ou resposta. Normalmente, armazenam, processam ou gerem operações criptográficas ou dados sensíveis, como credenciais de identidade ou credenciais de pagamento. Os elementos seguros são concebidos para assegurar a proteção de, pelo menos, nível AVA_VAN.4, tal como estabelecido nos Critérios Comuns ou na Metodologia Comum de Avaliação. Podem ser silício discreto ou estar integrados em sistemas num chipe (SoC). Os elementos seguros podem integrar um ambiente de aplicação ou um sistema operativo e incluir uma ou mais aplicações. Esta categoria inclui, entre outros, os módulos de plataformas de confiança e o cartão de circuito integrado universal embutido.
	Os cartões inteligentes ou dispositivos semelhantes são elementos seguros integrados num material de suporte, como plástico ou madeira, com a forma de um cartão, ou elementos seguros integrados em materiais de suporte com outras formas. Esta categoria inclui, entre outros, os documentos de identidade e de viagem, os cartões de assinatura qualificados, os cartões de circuito integrado universais substituíveis, os cartões de pagamento físicos, os cartões de acesso físicos, os cartões tacográficos digitais ou as braceletes de pulso com elementos seguros integrados para pagamento.

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