2024/3144

19.12.2024

REGULAMENTO DE EXECUÇÃO (UE) 2024/3144 DA COMISSÃO

de 18 de dezembro de 2024

que altera o Regulamento de Execução (UE) 2024/482 no respeitante às normas internacionais aplicáveis e que retifica esse regulamento de execução

(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) 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) ([1]), nomeadamente o artigo 49.º, n.º 7,

Considerando o seguinte:

(1) O Regulamento de Execução (UE) 2024/482 da Comissão ([2]) especifica as funções, regras e obrigações, bem como a estrutura do sistema europeu de certificação da cibersegurança baseado nos Critérios Comuns (EUCC), em conformidade com o enquadramento europeu para a certificação da cibersegurança estabelecido no Regulamento (UE) 2019/881.

(2) O Regulamento de Execução (UE) 2024/482 baseia-se em normas internacionais estabelecidas, a saber, os Critérios Comuns e a Metodologia Comum de Avaliação mantidos pela Organização Internacional de Normalização (ISO) e pela Comissão Eletrotécnica Internacional (IEC). O Regulamento de Execução (UE) 2024/482 faz referência às normas ISO/IEC, mas não especifica a versão aplicável dessas normas. Por conseguinte, há que especificar que versão das normas se aplica aos certificados emitidos ao abrigo do EUCC.

(3) As organizações governamentais que contribuíram para o desenvolvimento dos Critérios Comuns e da Metodologia Comum de Avaliação por meio do Acordo de Reconhecimento de Certificados de Critérios Comuns no domínio da Segurança das TI (ARCC) são cotitulares, juntamente com a ISO/IEC, dos direitos de autor sobre os mesmos. Essas organizações governamentais conservam o respetivo direito de utilização. Tendo em conta a importância desses documentos decorrentes do ARCC, é conveniente que também eles constituam uma base para a certificação ao abrigo do EUCC.

(4) As normas dos Critérios Comuns e da Metodologia Comum de Avaliação estão sujeitas a interpretações feitas pelo ARCC que facilitam a aplicação das mesmas e que podem ser tidas em conta pelos centros de avaliação da segurança das tecnologias da informação (ITSEF) e pelos organismos de certificação.

(5) As normas internacionais relativas aos Critérios Comuns podem ser objeto de atualizações. Para assegurar uma transição ordenada e atempada, é conveniente definir regras de transição para dar aos vendedores, aos ITSEF e aos organismos de certificação, bem como a outros intervenientes relevantes, tempo suficiente para procederem aos ajustamentos necessários. Essas regras de transição devem alinhar-se, conforme adequado, pelas práticas mundiais, como as estabelecidas pelo ARCC.

([1]) JO L 151 de 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.

([2]) 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).

(6) O Regulamento de Execução (UE) 2024/482 não especifica até quando a certificação de um produto de TIC se pode basear nas versões anteriores das normas dos Critérios Comuns e da Metodologia Comum de Avaliação. Os domínios técnicos e os perfis de proteção enumerados nos anexos I, II e III do referido regulamento de execução baseiam-se em versões anteriores das normas ISO/IEC 15408 e 18045. O Regulamento de Execução (UE) 2024/482 deve, por conseguinte, especificar em que circunstâncias a versão anterior dos Critérios Comuns e da Metodologia Comum de Avaliação continua a ser aplicável e como se procederá à transição para a versão mais recente das normas internacionais.

(7) Durante o período de transição, as partes interessadas devem dar prioridade à atualização dos domínios técnicos e dos perfis de proteção pertinentes. O Regulamento de Execução (UE) 2024/482 deve prever que as metas de segurança baseadas numa versão anterior das normas sejam aceites até 31 de dezembro de 2027, em consonância com a política de transição adotada pelo ARCC. No entanto, importa salientar que a política de transição do ARCC abrange avaliações iniciais de produtos e perfis de proteção com início, no máximo, em 30 de junho de 2024, data em que o EUCC ainda não era aplicável. Além disso, em conformidade com a política de transição do ARCC, o Regulamento de Execução (UE) 2024/482 deve prever que sejam aceites até 31 de dezembro de 2027 metas de segurança conformes com esse regulamento de execução que declarem a conformidade com perfis de proteção baseados numa versão anterior das normas. Acresce que, se for emitido um novo certificado ao abrigo do Regulamento de Execução (UE) 2024/482 no contexto de um processo de revisão de um certificado nacional que tenha início num prazo de dois anos a contar da emissão do certificado inicial, deve ser possível utilizar uma versão anterior das normas. Tal não será relevante no caso de um processo de revisão que não exija a emissão de um novo certificado ao abrigo do Regulamento de Execução (UE) 2024/482 e caso o certificado permaneça válido.

(8) A fim de assegurar uma transição ordenada para a versão mais recente das normas, o Regulamento de Execução (UE) 2024/482 deve prever regras de transição específicas e continuar a permitir a emissão de certificados ao abrigo desse regulamento de execução que declarem a conformidade com perfis de proteção baseados em versões anteriores das normas publicadas pelo ARCC, sempre que a legislação da União exija a utilização de tais perfis de proteção. É o caso do Regulamento de Execução (UE) 2016/799 da Comissão ([3]), bem como do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho ([4]) e da Decisão de Execução (UE) 2016/650 da Comissão ([5]).

(9) O anexo I do Regulamento de Execução (UE) 2024/482 enumera documentos sobre o estado da arte aplicáveis à avaliação de produtos de TIC e perfis de proteção. Todavia, não especifica a versão dos documentos. Há, pois, que especificar que versão dos documentos se aplica aos certificados emitidos ao abrigo do EUCC. Essas versões baseiam-se em documentos aprovados pelo Grupo Europeu para a Certificação da Cibersegurança (GECC), tendo sido objeto de uma análise mais aprofundada para a sua inclusão no EUCC. Além disso, o anexo I deve ser alterado de modo a incluir documentos atualizados e novos documentos sobre o estado da arte na sequência da sua aprovação pelo GECC, assegurando assim uma acreditação uniforme dos organismos de avaliação da conformidade no âmbito do EUCC. Os requisitos de acreditação relacionados com a acreditação de ITSEF devem ser atualizados para clarificar a aplicação dos critérios de independência e imparcialidade e deve ser estabelecido um novo documento sobre o estado da arte para a acreditação de organismos de certificação.

(10) Os documentos sobre o estado da arte poderão ser acrescentados ao EUCC ou ser objeto de atualizações no contexto das suas atividades de manutenção. No caso de documentos sobre o estado da arte novos ou atualizados, poderá ser necessário estabelecer regras de transição adequadas para permitir que os vendedores, os ITSEF, os organismos de certificação e outras partes interessadas procedam aos ajustamentos necessários. Para a atualização do documento sobre o estado da arte relacionado com a acreditação de ITSEF, o documento atualizado só deve aplicar-se às acreditações emitidas antes de 8 de julho de 2025 quando as mesmas forem revistas, por exemplo no contexto de um procedimento de avaliação ou reavaliação. Além disso, o documento atualizado deve aplicar-se a todas as acreditações de ITSEF emitidas após 8 de julho de 2025.

([3]) Regulamento de Execução (UE) 2016/799 da Comissão, de 18 de março de 2016, que dá execução ao Regulamento (UE) n.º 165/2014 do Parlamento Europeu e do Conselho que estabelece os requisitos para construção, ensaio, instalação, funcionamento e reparação de tacógrafos e seus componentes (JO L 139 de 26.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

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

([5]) Decisão de Execução (UE) 2016/650 da Comissão, de 25 de abril de 2016, que estabelece normas para a avaliação da segurança dos dispositivos qualificados de criação de assinaturas e selos nos termos dos artigos 30.º, n.º 3, e 39.º, n.º 2, do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno (JO L 109 de 26.4.2016, p. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).

(11) São feitas outras retificações dos artigos 5.º, 8.º, 16.º, 29.º e 44.º e do anexo IV do Regulamento de Execução (UE) 2024/482 que contribuem para assegurar uma redação uniforme e uma interpretação jurídica clara.

(12) As regras relativas às notificações dos organismos de avaliação da conformidade devem ser estabelecidas de forma transversal a todos os sistemas abrangidos pelo enquadramento europeu para a certificação da cibersegurança. O Regulamento de Execução (UE) 2024/3143 da Comissão ([6]) abarca essas regras de notificação. Os artigos 23.º e 24.º do Regulamento de Execução (UE) 2024/482 devem, portanto, ser suprimidos a partir da data de aplicação do Regulamento de Execução (UE) 2024/3143.

(13) O Regulamento de Execução (UE) 2024/482 deve, por conseguinte, ser alterado e retificado em conformidade.

(14) As medidas previstas no presente regulamento estão em conformidade com o parecer do comité criado pelo artigo 66.º do Regulamento (UE) 2019/881,

ADOTARAM O PRESENTE REGULAMENTO:

Artigo 1.º

O Regulamento de Execução (UE) 2024/482 é alterado do seguinte modo:

(1) No artigo 2.º, os pontos 1 e 2 passam a ter a seguinte redação:

«(1) "Critérios Comuns", os Critérios Comuns para a Avaliação da Segurança das Tecnologias da Informação, estabelecidos na norma ISO/IEC 15408-1:2022, ISO/IEC 15408-2:2022, ISO/IEC 15408-3:2022, ISO/IEC 15408-4:2022 ou ISO/IEC 15408-5:2022, ou estabelecidos nos Critérios Comuns para a Avaliação da Segurança das Tecnologias da Informação, versão CC:2022, partes 1 a 5, publicados pelos participantes no Acordo de Reconhecimento de Certificados de Critérios Comuns no domínio da Segurança das TI;

(2) "Metodologia Comum de Avaliação", a Metodologia Comum de Avaliação da Segurança das Tecnologias da Informação, estabelecida na norma ISO/IEC 18045:2022, ou a Metodologia Comum de Avaliação da Segurança das Tecnologias da Informação, versão CEM:2022, publicada pelos participantes no Acordo de Reconhecimento de Certificados de Critérios Comuns no domínio da Segurança das TI;»;

(2) O artigo 3.º passa a ter a seguinte redação:

«*Artigo 3.º*

Normas de avaliação

1. Às avaliações efetuadas no âmbito do sistema EUCC aplicam-se as seguintes normas:

a) Os Critérios Comuns;

b) A Metodologia Comum de Avaliação.

2. Até 31 de dezembro de 2027, podem ser emitidos certificados ao abrigo do sistema EUCC que apliquem uma das seguintes normas:

a) ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008 ou ISO/IEC 15408-3:2008;

b) Critérios Comuns para a Avaliação da Segurança das Tecnologias da Informação, versão 3.1, revisão 5, publicados pelos participantes no Acordo de Reconhecimento de Certificados de Critérios Comuns no domínio da Segurança das TI;

([6]) Regulamento de Execução (UE) 2024/3143 da Comissão, de 18 de dezembro de 2024, que estabelece as circunstâncias, os formatos e os procedimentos das notificações nos termos do artigo 61.º, n.º 5, do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação (JO L, 2024/3143, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3143/oj).

c) ISO/IEC 18045/2008;

d) Metodologia Comum de Avaliação da Segurança das Tecnologias da Informação, revisão 5, versão 3.1, publicada pelos participantes no Acordo de Reconhecimento de Certificados de Critérios Comuns no domínio da Segurança das TI.

3. Até 31 de dezembro de 2027, podem ser emitidos ao abrigo do sistema EUCC certificados que apliquem as normas referidas no n.º 1 que declarem a conformidade com um perfil de proteção que tenha aplicado as normas enumeradas no n.º 2.

4. Também podem ser emitidos ao abrigo do sistema EUCC certificados que apliquem as normas referidas no n.º 1 que declarem a conformidade com um perfil de proteção que tenha aplicado uma das normas que se seguem, contanto que a utilização desse perfil de proteção seja exigida nos termos do Regulamento de Execução (UE) 2016/799 da Comissão (*), do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho (**) ou da Decisão de Execução (UE) 2016/650 da Comissão (***):

a) Critérios Comuns para a Avaliação da Segurança das Tecnologias da Informação, versão 3.1, revisões 1 a 4, publicados pelos participantes no Acordo de Reconhecimento de Certificados de Critérios Comuns no domínio da Segurança das TI;

b) Metodologia Comum de Avaliação da Segurança das Tecnologias da Informação, versão 3.1, revisões 1 a 4, publicada pelos participantes no Acordo de Reconhecimento de Certificados de Critérios Comuns no domínio da Segurança das TI.

(*) Regulamento de Execução (UE) 2016/799 da Comissão, de 18 de março de 2016, que dá execução ao Regulamento (UE) n.º 165/2014 do Parlamento Europeu e do Conselho que estabelece os requisitos para construção, ensaio, instalação, funcionamento e reparação de tacógrafos e seus componentes (JO L 139 de 26.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

(**) Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE (JO L 257 de 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

(***) Decisão de Execução (UE) 2016/650 da Comissão, de 25 de abril de 2016, que estabelece normas para a avaliação da segurança dos dispositivos qualificados de criação de assinaturas e selos nos termos dos artigos 30.º, n.º 3, e 39.º, n.º 2, do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno (JO L 109 de 26.4.2016, p. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).»;

(3) No capítulo IV, é inserido o seguinte artigo 20.º-A:

«*Artigo 20.º-A*

Especificação dos requisitos de acreditação dos organismos de avaliação da conformidade

A acreditação dos organismos de avaliação da conformidade deve ter em conta a especificação dos requisitos de acreditação de organismos de certificação e ITSEF estabelecidos nos documentos sobre o estado da arte aplicáveis enumerados no anexo I, ponto 2.»;

(4) São suprimidos os artigos 23.º e 24.º;

(5) Ao artigo 48.º é aditado o seguinte n.º 4:

«4. Salvo disposição em contrário no anexo I ou II, os documentos sobre o estado da arte são aplicáveis a partir da data de aplicação do ato modificativo pelo qual foram incorporados no anexo I ou II.»;

(6) Ao artigo 49.º é aditado o seguinte n.º 4:

«4. Quando a revisão a que se refere o n.º 3 for efetuada no prazo de dois anos a contar da emissão do certificado inicial e se essa revisão conduzir à emissão de um novo certificado em conformidade com o presente regulamento, podem ser aplicadas as normas enumeradas no artigo 3.º, n.º 2. Deve entender-se por data de emissão do certificado inicial a data de emissão do último certificado para um produto de TIC ou perfil de proteção em que se baseia a certificação atual.»;

(7) O anexo I é substituído pelo texto constante do anexo I do presente regulamento;

(8) O anexo IV é alterado em conformidade com o anexo II do presente regulamento.

Artigo 2.º

O Regulamento de Execução (UE) 2024/482 é retificado do seguinte modo:

(1) No artigo 5.º, n.º 1, a alínea b) passa a ter a seguinte redação:

«b) Declarando a conformidade com um perfil de proteção certificado como parte do processo de TIC, se o produto de TIC pertencer à categoria de produtos de TIC abrangida por esse perfil de proteção.»;

(2) O artigo 8.º é retificado do seguinte modo:

a) O título passa a ter a seguinte redação:

«Informações necessárias para a certificação e a avaliação»;

b) O n.º 1 passa a ter a seguinte redação:

«1. O requerente da certificação no âmbito do EUCC deve fornecer ou de outro modo disponibilizar ao organismo de certificação e ao ITSEF todas as informações necessárias para as atividades de certificação e avaliação.»;

(3) O artigo 16.º passa a ter a seguinte redação:

«*Artigo 16.º*

Informações necessárias para a certificação e a avaliação de perfis de proteção

O requerente da certificação de um perfil de proteção deve fornecer ou de outro modo disponibilizar ao organismo de certificação e ao ITSEF todas as informações necessárias para as atividades de certificação e avaliação de maneira completa e correta. É aplicável, *mutatis mutandis*, o artigo 8.º, n.ºs 2, 3, 4 e 7.»;

(4) No artigo 17.º, é suprimido o n.º 1;

(5) No artigo 29.º, o n.º 2 passa a ter a seguinte redação:

«2. Se o titular do certificado EUCC não propuser medidas corretivas adequadas no prazo referido no n.º 1, o certificado é suspenso, em conformidade com o artigo 30.º, ou retirado, em conformidade com o artigo 14.º ou 20.º.».

Artigo 3.º

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

O artigo 1.º, ponto 4, é aplicável a partir de 8 de janeiro de 2025.

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

Feito em Bruxelas, em 18 de dezembro de 2024.

Pela Comissão
A Presidente
Ursula VON DER LEYEN

ANEXO I

«*ANEXO I*

Documentos sobre o estado da arte que apoiam os domínios técnicos e outros documentos sobre o estado da arte

1. Documentos sobre o estado da arte que apoiam os domínios técnicos nos níveis AVA_VAN 4 ou 5:

   a) Os seguintes documentos relativos à avaliação harmonizada do domínio técnico "cartões inteligentes e dispositivos similares":

      1) "Minimum ITSEF requirements for security evaluations of smart cards and similar devices" (Requisitos mínimos dos ITSEF para as avaliações de segurança de cartões inteligentes e dispositivos similares), versão 1.1;

      2) "Minimum Site Security Requirements" (Requisitos mínimos de segurança dos sítios), versão 1.1;

      3) "Application of Common Criteria to integrated circuits" (Aplicação dos Critérios Comuns aos circuitos integrados), versão 1.1;

      4) "Security Architecture requirements (ADV_ARC) for smart cards and similar devices" [Requisitos de arquitetura de segurança (ADV_ARC) para cartões inteligentes e dispositivos similares], versão 1.1;

      5) "Certification of 'open' smart card products" (Certificação de produtos de cartões inteligentes "abertos"), versão 1.1;

      6) "Composite product evaluation for smart cards and similar devices" (Avaliação de produtos compostos para cartões inteligentes e dispositivos similares), versão 1.1;

      7) "Application of Attack Potential to Smartcards and Similar Devices" (Aplicação do potencial de ataque aos cartões inteligentes e dispositivos similares), versão 1.2.

   b) Os seguintes documentos relativos à avaliação harmonizada do domínio técnico "dispositivos de *hardware* com caixas de segurança":

      1) "Minimum ITSEF requirements for security evaluations of hardware devices with security boxes" (Requisitos mínimos dos ITSEF para as avaliações de segurança de dispositivos de *hardware* com caixas de segurança), versão 1.1;

      2) "Minimum Site Security Requirements" (Requisitos mínimos de segurança dos sítios), versão 1.1;

      3) "Application of Attack Potential to hardware devices with security boxes" (Aplicação do potencial de ataque a dispositivos de *hardware* com caixas de segurança), versão 1.2.

2. Documentos sobre o estado da arte relativos à acreditação harmonizada dos organismos de avaliação da conformidade:

   a) "Accreditation of ITSEFs for the EUCC" (Acreditação dos ITSEF para o EUCC), versão 1.1 para acreditações emitidas antes de 8 de julho de 2025.

   b) "Accreditation of ITSEFs for the EUCC" (Acreditação dos ITSEF para o EUCC), versão 1.6c, para acreditações emitidas pela primeira vez ou revistas após 8 de julho de 2025.

   c) "Accreditation of CBs for the EUCC" (Acreditação dos OC para o EUCC), versão 1.6b.»»

ANEXO II

No anexo IV do Regulamento de Execução (UE) 2024/482, secção IV.3, os pontos 5 e 6 passam a ter a seguinte redação:

«5. Se o organismo de certificação confirmar as alterações como menores, não é emitido um novo certificado para o produto de TIC modificado e é elaborado um relatório de manutenção do relatório de certificação inicial.

O relatório de manutenção deve ser incluído como um subconjunto do relatório de análise de impacto, contendo as seguintes secções:

a) Introdução;

b) Descrição das alterações;

c) Elementos de prova do criador afetados.

6. O relatório de manutenção a que se refere o ponto 5 deve ser fornecido à ENISA para publicação no seu sítio Web dedicado à certificação da cibersegurança.»