2025/2531

17.12.2025

REGULAMENTO DE EXECUÇÃO (UE) 2025/2531 DA COMISSÃO

de 16 de dezembro de 2025

que estabelece as regras de execução do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho no respeitante às normas de referência e especificações para livros-razão eletrónicos qualificados

A COMISSÃO EUROPEIA,

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

Tendo em conta o 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 ([1]), nomeadamente o artigo 45.º-L, n.º 3,

Considerando o seguinte:

(1) Por força do Regulamento (UE) 2024/1183 do Parlamento Europeu e do Conselho ([2]), foi introduzida no Regulamento (UE) n.º 910/2014 uma lista de novos serviços de confiança e de serviços de confiança qualificados, incluindo o registo de dados eletrónicos num livro-razão eletrónico qualificado. Importa que a Comissão estabeleça uma lista de normas de referência e, se necessário, especificações para esses serviços.

(2) Um livro-razão eletrónico consiste numa sequência de registos de dados eletrónicos destinada a assegurar a integridade desses registos de dados e a exatidão da ordem cronológica desses registos. A fim de assegurar que o registo de dados num livro-razão eletrónico qualificado é ordenado cronologicamente, coerente e fiável, é necessário estabelecer um conjunto comum de especificações para o registo de dados eletrónicos num livro-razão eletrónico qualificado.

(3) A presunção de conformidade estabelecida no artigo 45.º-L, n.º 2, do Regulamento (UE) n.º 910/2014 só deve aplicar-se se os serviços de confiança qualificados para o registo de dados eletrónicos num livro-razão eletrónico qualificado cumprirem as normas estabelecidas no presente regulamento. Estas normas devem refletir as práticas estabelecidas e ser amplamente reconhecidas nos setores pertinentes. Devem igualmente ser adaptadas de modo a incluir controlos adicionais que garantam a segurança e a fiabilidade do serviço de confiança qualificado.

(4) Se um prestador de serviços de confiança cumprir os requisitos estabelecidos no anexo do presente regulamento, as entidades supervisoras devem presumir a conformidade com os requisitos pertinentes do Regulamento (UE) n.º 910/2014 e ter devidamente em conta essa presunção para conceder ou confirmar o estatuto de qualificado do serviço de confiança. No entanto, um prestador qualificado de serviços de confiança pode continuar a invocar outras práticas para demonstrar o cumprimento dos requisitos do Regulamento (UE) n.º 910/2014.

(5) A Comissão avalia periodicamente as novas tecnologias, práticas, normas ou especificações técnicas. Em conformidade com o considerando 75 do Regulamento (UE) 2024/1183, a Comissão deve rever e, se necessário, atualizar o presente regulamento, a fim de assegurar que o mesmo acompanha a evolução mundial, as novas tecnologias, práticas, normas ou especificações técnicas e de seguir as boas práticas no mercado interno.

([1]) JO L 257 de 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Regulamento (UE) 2024/1183 do Parlamento Europeu e do Conselho, de 11 de abril de 2024, que altera o Regulamento (UE) n.º 910/2014 no respeitante à criação do Regime Europeu para a Identidade Digital (JO L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(6) O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ([3]) e, se for caso disso, a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho ([4]) são aplicáveis às atividades de tratamento de dados pessoais nos termos do presente regulamento, tendo igualmente em conta as *Guidelines 02/2025 on processing of personal data through blockchain technologies* [Diretrizes 02/2025 relativas ao tratamento de dados pessoais por meio de tecnologias de cadeia de blocos] do Comité Europeu para a Proteção de Dados ([5]).

(7) A Autoridade Europeia para a Proteção de Dados foi consultada nos termos do artigo 42.º, n.º 1, do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho ([6]) e emitiu parecer em 21 de outubro de 2025 ([7]).

(8) As medidas previstas no presente regulamento estão em conformidade com o parecer do comité instituído pelo artigo 48.º do Regulamento (UE) n.º 910/2014,

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

Normas de referência e especificações

As normas de referência e especificações a que se refere o artigo 45.º-L, n.º 3, do Regulamento (UE) n.º 910/2014 são estabelecidas, para os livros-razão eletrónicos qualificados, no anexo do presente regulamento.

Artigo 2.º

Entrada em vigor

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 16 de dezembro de 2025.

Pela Comissão
A Presidente
Ursula VON DER LEYEN

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

([4]) Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO L 201 de 31.7.2002, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) edpb_guidelines_202502_blockchain_en.pdf.

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

([7]) EDPS Formal comments on the draft Implementing Regulation laying down rules for the application of Regulation (EU) No 910/2014 as regards reference standards and specifications for qualified electronic ledgers [não traduzido para português].

ANEXO

Lista de especificações técnicas e normas de referência para os livros-razão eletrónicos distribuídos qualificados

1. Para efeitos do presente regulamento, entende-se por:

   a) «Caráter definitivo», o estado de um registo de dados de um livro-razão eletrónico que se tornou irreversível e não pode ser modificado nem removido;

   b) «Livro-razão eletrónico distribuído», um livro-razão eletrónico partilhado por um conjunto de nós de livro-razão eletrónico distribuído e sincronizado entre esses nós por meio de um mecanismo de consenso;

   c) «Nó de livro-razão eletrónico distribuído», um dispositivo ou processo que faz parte de uma rede de livros-razão eletrónicos distribuídos e que armazena uma cópia completa ou parcial dos registos de dados de um livro-razão eletrónico;

   d) «Rede de livros-razão eletrónicos distribuídos», uma rede de nós de livro-razão eletrónico distribuído que constitui um sistema de livro-razão eletrónico distribuído;

   e) «Sistema de livro-razão eletrónico distribuído», um sistema que implementa um livro-razão eletrónico distribuído;

   f) «Consenso», um acordo entre nós de livro-razão eletrónico distribuído sobre a validade das transações e a manutenção de um conjunto coerente e ordenado de transações validadas no sistema de livro-razão eletrónico distribuído;

   g) «Mecanismo de consenso», o conjunto de regras e procedimentos pelos quais se chega a um consenso;

   h) «Regras de governação», o conjunto de protocolos, políticas e mecanismos que determinam o funcionamento do sistema de livro-razão eletrónico distribuído, a forma como os dados são validados e adicionados a um livro-razão eletrónico e a forma de interação dos participantes;

   i) «Transação», a unidade mais pequena de um processo de trabalho de um livro-razão eletrónico;

   j) «Processo de trabalho», uma ou mais sequências de ações necessárias para produzir um resultado conforme com as regras de governação de um livro-razão eletrónico;

   k) «Transação validada», uma transação para a qual a integridade, a autenticidade e as condições específicas do protocolo necessárias foram verificadas em conformidade com as regras de governação do sistema de livro-razão eletrónico distribuído;

   l) «Ligação criptográfica», uma referência a dados que é estabelecida utilizando técnicas criptográficas adequadas para assegurar a integridade, a autenticidade ou a rastreabilidade dos dados referenciados e a sequência correta dos registos de dados;

   m) «Relatório de livro-razão», uma apresentação estruturada de informações verificáveis extraídas dos registos de dados de um livro-razão eletrónico e que fornece informações sobre atividades específicas, estados ou conformidade com regras predefinidas;

   n) «Fornecedor de livro-razão eletrónico qualificado», um prestador qualificado de serviços de confiança que presta um serviço de confiança qualificado que consiste no registo de dados num livro-razão eletrónico qualificado;

   o) «Livro-razão eletrónico distribuído qualificado», um livro-razão eletrónico distribuído que cumpre os requisitos de um livro-razão eletrónico qualificado.

2. Sempre que o prestador qualificado de serviços de confiança necessitar de elaborar um relatório de livro-razão, deve fazê-lo de forma automatizada.

3. Os fornecedores de livros-razão eletrónicos qualificados devem criar, registar dados eletrónicos, atualizar e manter um livro-razão eletrónico qualificado em conformidade com as especificações estabelecidas:

   a) Para todos os fornecedores de livros-razão eletrónicos qualificados, ETSI EN 319 401 V3.1.1 (2024-06), com as seguintes adaptações:

      — 2.1 Referências normativas:

        [1] Grupo Europeu para a Certificação da Cibersegurança, subgrupo para a criptografia: «Agreed Cryptographic Mechanisms» [Mecanismos criptográficos acordados], publicado pela Agência da União Europeia para a Cibersegurança (ENISA);

[2] RFC 7515 do IETF (maio de 2015): «JSON Web Signature (JWS)» [Assinatura Web JSON];

[3] FIPS PUB 140-3 (2019) «Security Requirements for Cryptographic Modules» [Requisitos de segurança para módulos criptográficos];

[4] 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);

[5] 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;

[6] ISO/IEC 15408:2022 (partes 1 a 5): «Information security, cybersecurity and privacy protection — Evaluation criteria for IT security» [Segurança da informação, cibersegurança e proteção da privacidade — Critérios de avaliação da segurança informática].

— 6.1. Declaração de práticas dos serviços de confiança:

  — REQ-6.1-12 A declaração de práticas do livro-razão eletrónico deve incluir, pelo menos, as seguintes informações:

    — as capacidades funcionais e técnicas da plataforma de livro-razão eletrónico e a respetiva utilização ao longo da prestação do serviço de registo de dados num livro-razão eletrónico qualificado como serviço de confiança qualificado,

    — os mecanismos específicos de autenticação da origem dos dados utilizados na prestação do serviço,

    — os mecanismos específicos de ordenação cronológica sequencial utilizados na prestação do serviço,

    — se for caso disso, a ligação criptográfica utilizada para assegurar a sequência dos registos de dados,

    — se for caso disso, o mecanismo de consenso que assegura o caráter definitivo e a integridade dos registos de dados e das transações armazenados no livro-razão, incluindo qualquer período de precaução até se atingir o caráter definitivo e a integridade,

    — os mecanismos específicos de integridade dos dados utilizados na prestação do serviço.

  — 6.2. Termos e condições:

    — REQ-6.2-03 Os assinantes e os utilizadores do serviço de confiança devem ser informados, de forma clara, exaustiva e facilmente acessível, num espaço de acesso público e individualmente, dos termos e condições exatos, incluindo os itens enumerados acima, antes de estabelecerem uma relação contratual.

  — 6.3. Política de segurança da informação:

    — REQ-6.3-04X O prestador de serviços de confiança (TSP) deve estabelecer procedimentos para notificar a entidade supervisora de quaisquer alterações da prestação do serviço de confiança, em conformidade com os requisitos operacionais e as disposições legislativas e regulamentares aplicáveis. O TSP deve notificar a entidade supervisora pelo menos:

      — um mês antes da implementação de qualquer alteração,

      — três meses antes da cessação prevista da prestação de um serviço de confiança.

  — 7.2. Recursos humanos:

    — REQ-7.2-04X O pessoal do TSP com funções de confiança deve ser capaz de cumprir o requisito de dispor de conhecimentos especializados, experiência e qualificações adquiridos por meio de formação formal e credenciais, de experiência ou de uma combinação de ambas.

— REQ-7.2-05X Isto inclui atualizações regulares (pelo menos a cada 12 meses) sobre as novas ameaças e as atuais práticas de segurança.

— 7.5. Controlos criptográficos:

— REQ-7.5-01X Devem existir controlos de segurança adequados para a gestão de quaisquer chaves criptográficas, algoritmos criptográficos e dispositivos criptográficos ao longo do seu ciclo de vida, seguindo, se for caso disso, uma abordagem de agilidade criptográfica.

— REQ-7.5-02 Para efeitos da prestação dos respetivos serviços de confiança, o TSP deve selecionar e utilizar técnicas criptográficas adequadas conformes com os mecanismos criptográficos acordados, aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela ENISA [1].

Em particular:

— REQ-7.5-03 Os fornecedores de livros-razão eletrónicos qualificados devem estabelecer a origem dos registos de dados no livro-razão eletrónico. Para o efeito, devem utilizar assinaturas eletrónicas avançadas baseadas em certificados qualificados ou selos eletrónicos avançados baseados em certificados qualificados criados pelos utentes do serviço em conformidade com as seguintes normas e especificações:

a) ETSI EN 319 122-1 V1.3.1 (2023-06). «Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures» [Assinaturas eletrónicas e infraestruturas (ESI); assinaturas digitais CAdES; parte 1: blocos de construção e assinaturas de base CAdES];

b) ETSI EN 319 132-1 V1.3.1 (2024-07). «Electronic Signatures and Trust Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures» [Assinaturas eletrónicas e infraestruturas de confiança (ESI); assinaturas digitais XAdES; parte 1: blocos de construção e assinaturas de base XAdES];

c) ETSI TS 119 182-1 V1.2.1 (2024-07). «Electronic Signatures and Trust Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures» [Assinaturas eletrónicas e infraestruturas de confiança (ESI); assinaturas digitais JAdES; parte 1: blocos de construção e assinaturas de base JAdES], com a seguinte adaptação:

— 5.1.8 Parâmetro do cabeçalho x5c (cadeia de certificados X.509)

— o parâmetro do cabeçalho x5c definido na cláusula 4.1.6 do RFC 7515 do IETF [2] deve estar presente na assinatura JAdES, quer seja como um parâmetro do cabeçalho assinado ou não assinado,

— o parâmetro do cabeçalho x5c deve ter a semântica especificada no RFC 7515 do IETF [2], cláusula 4.1.6,

— o parâmetro do cabeçalho x5c deve ter a sintaxe especificada no RFC 7515 do IETF [2], cláusula 4.1.6.

— REQ-7.5-04: os fornecedores de livros-razão eletrónicos qualificados devem assegurar a ordem cronológica única e sequencial dos registos de dados no livro-razão eletrónico. Para o efeito, devem utilizar ligações criptográficas, baseadas em listas ou árvores de dispersão, utilizando funções de dispersão criptográficas, em conformidade com as seguintes especificações e normas:

a) SHA-256 ou um tamanho maior do valor de dispersão de saída, em conformidade com os mecanismos criptográficos acordados aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela ENISA [1];

b) SHA3-256 ou um tamanho maior do valor de dispersão de saída, em conformidade com os mecanismos criptográficos acordados aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela ENISA [1];

Em alternativa, sempre que utilizarem o registo do tempo para assegurar a ordem cronológica única e sequencial dos registos de dados no livro-razão eletrónico, os fornecedores de livros-razão eletrónicos qualificados devem utilizar selos temporais qualificados.

— REQ-7.5-05 Os fornecedores de livros-razão eletrónicos qualificados devem assegurar a integridade dos registos de dados inscritos num livro-razão eletrónico qualificado. Para o efeito, devem utilizar assinaturas eletrónicas avançadas baseadas em certificados qualificados ou selos eletrónicos avançados baseados em certificados qualificados, em conformidade com as seguintes normas e especificações:

a) Qualquer formato de assinatura ou de selo conforme com os mecanismos criptográficos acordados, aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela ENISA [1];

b) SHA-256 ou um tamanho maior do valor de dispersão de saída, em conformidade com os mecanismos criptográficos acordados aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela ENISA [1];

c) SHA3-256 ou um tamanho maior do valor de dispersão de saída, em conformidade com os mecanismos criptográficos acordados aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela ENISA [1];

d) Os fornecedores de livros-razão eletrónicos qualificados devem assegurar a detetabilidade imediata de qualquer alteração posterior dos dados registados num livro-razão eletrónico qualificado.

— REQ-7.5-06 Sempre que sejam utilizados mecanismos de assinatura digital, as chaves de assinatura privadas do fornecedor de livro-razão eletrónico qualificado devem ser mantidas e utilizadas num dispositivo criptográfico seguro que seja um sistema fiável certificado em conformidade com:

a) Os Critérios Comuns para a Avaliação da Segurança das Tecnologias da Informação, estabelecidos na norma ISO/IEC 15408 ([1]) [6] ou 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, e certificado com o nível EAL 4 ou superior; ou

b) O sistema europeu de certificação da cibersegurança baseado nos Critérios Comuns (EUCC) ([2]) ([3]) [4][5] e certificado com o nível EAL 4 ou superior; ou

c) Até 31.12.2030, FIPS PUB 140-3 ([4]) [3] nível 3.

Esta certificação refere-se a uma meta de segurança ou a um perfil de proteção, ou a uma documentação de segurança e conceção de módulos, que cumpra os requisitos do presente documento, com base numa análise de risco e tendo em conta as medidas de segurança físicas e outras medidas de segurança não técnicas;

Se o dispositivo criptográfico seguro possuir uma certificação EUCC [4][5], deve ser configurado e utilizado em conformidade com essa certificação.

([1]) ISO/IEC 15408:2022 (partes 1 a 5): «Information security, cybersecurity and privacy protection — Evaluation criteria for IT security» [Segurança da informação, cibersegurança e proteção da privacidade — Critérios de avaliação da segurança informática].

([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/2024/482/2025-01-08).

([3]) 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 (JO L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

([4]) FIPS PUB 140-3 (2019): «Security Requirements for Cryptographic Modules» (Requisitos de segurança para módulos criptográficos).

— 7.8. Segurança da rede:

— REQ-7.8-14X A análise das vulnerabilidades solicitada pelo REQ-7.8-13 deve ser efetuada, pelo menos, uma vez por trimestre;

— REQ-7.8-18X O teste de penetração solicitado pelo REQ-7.8-17X deve ser efetuado, pelo menos, uma vez por ano;

— REQ-7.8-21X: as barreiras de segurança são igualmente configuradas de modo a impedir todos os protocolos e acessos não necessários para a operação do TSP.

— 7.9.1. Monitorização e registo:

— REQ-7.9.1-02X As atividades de monitorização devem ter em conta o grau de sensibilidade de todas as informações recolhidas ou analisadas.

— 7.12. Cessação e planos de cessação do TSP

— REQ-7.12-02A O plano de cessação do TSP deve cumprir os requisitos estabelecidos nos atos de execução adotados nos termos do artigo 24.º, n.º 5, do Regulamento (UE) n.º 910/2014 [i.1].

b) Além disso, para todos os fornecedores de livros-razão eletrónicos qualificados que utilizam tecnologias de livro-razão eletrónico distribuído:

1) ISO 23257:2022 «Blockchain and distributed ledger technologies — Reference architecture» [Tecnologias de cadeia de blocos e de livro-razão distribuído — Arquitetura de referência], cláusula 9, que fornece uma descrição completa do sistema de tecnologias de livro-razão eletrónico distribuído, bem como da rede de tecnologias de livro-razão eletrónico distribuído e dos nós de tecnologias de livro-razão eletrónico distribuído correspondentes;

2) ISO/TS 23635:2022 «Blockchain and distributed ledger technologies — Guidelines for governance» [Tecnologias de cadeia de blocos e de livro-razão distribuído — Orientações para a governação], no que diz respeito a políticas e práticas escritas e acessíveis ao público relacionadas com a estrutura de governação do serviço de livro-razão eletrónico que prestam.