2025/2531

17.12.2025

REGLAMENTO DE EJECUCIÓN (UE) 2025/2531 DE LA COMISIÓN

de 16 de diciembre de 2025

por el que se establecen disposiciones de aplicación del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a las normas y especificaciones de referencia para los libros mayores electrónicos cualificados

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE ([1]), y en particular su artículo 45 *terdecies*, apartado 3,

Considerando lo siguiente:

(1) Mediante el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo ([2]), se introdujo en el Reglamento (UE) n.º 910/2014 una lista de nuevos servicios de confianza y servicios de confianza cualificados, incluido el registro de datos electrónicos en un libro mayor electrónico cualificado. La Comisión debe establecer una lista de normas de referencia y, cuando sea necesario, establecer especificaciones para dichos servicios.

(2) Un libro mayor electrónico es una secuencia de registros electrónicos de datos que garantiza la integridad de dichos registros de datos y la exactitud de su orden cronológico. A fin de garantizar que el registro de datos en un libro mayor electrónico cualificado se ordene cronológicamente y sea coherente y fiable, es necesario establecer un conjunto común de especificaciones para el registro de datos electrónicos en un libro mayor electrónico cualificado.

(3) La presunción de cumplimiento establecida en el artículo 45 *terdecies*, apartado 2, del Reglamento (UE) n.º 910/2014 solo debe aplicarse cuando los servicios de confianza cualificados para el registro de datos electrónicos en un libro mayor electrónico cualificado cumplan las normas establecidas en el presente Reglamento. Estas normas deben reflejar las prácticas establecidas y ser ampliamente aceptadas en los sectores pertinentes. Deben adaptarse para incluir controles adicionales que garanticen la seguridad y la fiabilidad del servicio de confianza cualificado.

(4) Si un prestador de servicios de confianza cumple los requisitos establecidos en el anexo del presente Reglamento, los organismos de supervisión deben presumir el cumplimiento de los requisitos pertinentes del Reglamento (UE) n.º 910/2014 y tener debidamente en cuenta dicha presunción para conceder o confirmar la cualificación del servicio de confianza. No obstante, un prestador cualificado de servicios de confianza puede seguir basándose en otras prácticas para demostrar el cumplimiento de los requisitos del Reglamento (UE) n.º 910/2014.

(5) La Comisión evalúa periódicamente las nuevas tecnologías, prácticas, normas y especificaciones técnicas. De conformidad con el considerando 75 del Reglamento (UE) 2024/1183, la Comisión debe revisar y, en caso necesario, actualizar el presente Reglamento para mantenerlo en consonancia con la evolución mundial, las nuevas tecnologías, prácticas, normas o especificaciones técnicas y seguir las mejores prácticas del mercado interior.

([1]) DO L 257 de 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital (DO L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(6) El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([3]) y, en su caso, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo ([4]) son aplicables a las actividades de tratamiento de datos personales en virtud del presente Reglamento, teniendo también en cuenta las «Directrices 02/2025 sobre el tratamiento de datos personales a través de tecnologías de cadena de bloque» del Comité Europeo de Protección de Datos ([5]).

(7) El Supervisor Europeo de Protección de Datos, al que se consultó de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo ([6]), emitió su dictamen el 21 de octubre de 2025 ([7]).

(8) Las medidas previstas en el presente Reglamento se ajustan al dictamen del comité establecido por el artículo 48 del Reglamento (UE) n.º 910/2014.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

Normas de referencia y especificaciones

Las normas y especificaciones de referencia a que se refiere el artículo 45 *terdecies*, apartado 3, del Reglamento (UE) n.º 910/2014 figuran, para los libros mayores electrónicos cualificados en el anexo del presente Reglamento.

Artículo 2

Entrada en vigor

El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el 16 de diciembre de 2025.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

([3]) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO 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]) Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DO 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 for qualified electronic ledgers [«Observaciones formales del SEPD sobre el proyecto de Reglamento de Ejecución por el que se establecen disposiciones de aplicación del Reglamento (UE) n.º 910/2014 en lo que respecta a las normas de referencia para los libros mayores electrónicos cualificados», documento en inglés].

ANEXO

Lista de especificaciones técnicas y normas de referencia para libros mayores electrónicos distribuidos cualificados

1. A los efectos del presente Reglamento, se entenderá por:

   a) «carácter definitivo»: el estado de un registro de datos de un libro mayor electrónico que se ha vuelto irreversible y no puede modificarse ni suprimirse;

   b) «libro mayor electrónico distribuido»: un libro mayor electrónico que se comparte entre un conjunto de nodos de libro mayor electrónico distribuido y que está sincronizado entre los nodos de libro mayor electrónico distribuido utilizando un mecanismo de consenso;

   c) «nodo de libro mayor electrónico distribuido»: dispositivo o proceso que forma parte de una red de libro mayor electrónico distribuido y almacena una copia completa o parcial de los registros de datos de un libro mayor electrónico;

   d) «red de libro mayor electrónico distribuido»: una red de nodos de libro mayor electrónico distribuido que constituye un sistema de libro mayor electrónico distribuido;

   e) «sistema de libro mayor electrónico distribuido»: sistema que implementa un libro mayor electrónico distribuido;

   f) «consenso»: acuerdo entre nodos de libro mayor electrónico distribuido sobre la validez de las transacciones y el mantenimiento de un conjunto coherente y ordenado de transacciones validadas en todo el sistema de libro mayor electrónico distribuido;

   g) «mecanismo de consenso»: el conjunto de normas y procedimientos mediante los cuales se alcanza un consenso;

   h) «normas reguladoras»: el conjunto de protocolos, políticas y mecanismos que dictan cómo funciona el sistema de libro mayor electrónico distribuido, cómo se validan los datos y se añaden a un libro mayor electrónico, y cómo interactúan los participantes;

   i) «transacción»: la unidad más pequeña de un proceso de trabajo en un libro mayor electrónico;

   j) «proceso de trabajo»: una o varias secuencias de acciones necesarias para producir un resultado que cumpla las normas que rigen un libro mayor electrónico;

   k) «transacción validada»: una transacción cuya integridad, autenticidad y condiciones específicas del protocolo requeridas han sido comprobadas de conformidad con las normas que rigen el sistema de libro mayor electrónico distribuido;

   l) «vínculo criptográfico»: referencia a datos que se establece utilizando técnicas criptográficas adecuadas para garantizar la integridad, autenticidad o trazabilidad de los datos referenciados y la secuencia correcta de registros de datos;

   m) «informe del libro mayor»: presentación estructurada de información verificable extraída de los registros de datos de un libro mayor electrónico, que proporciona información sobre actividades, estados o cumplimiento de normas predefinidas específicos;

   n) «prestador de un libro mayor electrónico cualificado»: un prestador cualificado de servicios de confianza que presta un servicio de confianza cualificado consistente en el registro de datos en un libro mayor electrónico cualificado;

   o) «libro mayor electrónico distribuido cualificado»: un libro mayor electrónico distribuido que cumple los requisitos de un libro mayor electrónico cualificado.

2. Cuando el prestador cualificado de servicios de confianza necesite elaborar un informe de registro, este se elaborará de manera automatizada.

3. Los prestadores de libros mayores electrónicos cualificados crearán un libro mayor electrónico cualificado, lo actualizarán y mantendrán, y registrarán datos electrónicos en dicho libro mayor, de conformidad con las especificaciones establecidas en:

   a) En el caso de todos los prestadores de libros mayores electrónicos cualificados, ETSI EN 319 401 v3.1.1 (2024-06) con las siguientes adaptaciones:

      — 2.1 Referencias normativas:

      [1] Grupo Europeo de Certificación de la Ciberseguridad, Subgrupo de Criptografía: «Agreed Cryptographic Mechanisms» («Mecanismos criptográficos acordados», documento en inglés) publicado por la Agencia de la Unión Europea para la Ciberseguridad («ENISA»).

[2] IETF RFC 7515 (mayo 2015): «JSON Web Signature (JWS)» [«Firma web JSON»].

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

[4] Reglamento de Ejecución (UE) 2024/482 de la Comisión, de 31 de enero de 2024, por el que se establecen disposiciones de aplicación del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo en lo concerniente a la adopción del esquema europeo de certificación de la ciberseguridad basado en los criterios comunes (EUCC).

[5] Reglamento de Ejecución (UE) 2024/3144 de la Comisión, de 18 de diciembre de 2024, por el que se modifica el Reglamento de Ejecución (UE) 2024/482 en lo que respecta a las normas internacionales aplicables y se corrige dicho Reglamento de Ejecución.

[6] ISO/IEC 15408:2022 (partes 1 a 5): «Seguridad de la información, ciberseguridad y protección de la privacidad. Criterios de evaluación para la seguridad de TI».

— 6.1 Declaración de prácticas del servicio de confianza:

  — REQ-6.1-12 La declaración de prácticas del libro mayor electrónico incluirá, como mínimo, la siguiente información:

    — las capacidades funcionales y técnicas de la plataforma de registro electrónico y su uso durante todo el proceso de registro de datos en un libro mayor electrónico cualificado como servicio de confianza cualificado;

    — los mecanismos específicos de autenticación del origen de los datos utilizados al prestar el servicio;

    — los mecanismos específicos de orden cronológico secuencial utilizados al prestar el servicio;

    — cuando proceda, el vínculo criptográfico utilizado para garantizar la secuencia de registros de datos;

    — cuando proceda, el mecanismo de consenso que garantice el carácter definitivo y la integridad de los registros de datos y las transacciones almacenados en el libro mayor, incluido cualquier período cautelar hasta que se consigan su carácter definitivo y su integridad;

    — los mecanismos específicos de integridad de los datos utilizados al prestar el servicio;

  — 6.2 Condiciones generales:

    — REQ-6.2-03 Los abonados y las partes que dependan del servicio de confianza serán informados, de manera clara, completa y fácilmente accesible, en un espacio de acceso público e individualmente, de las condiciones precisas, incluidos los elementos enumerados anteriormente, antes de entablar una relación contractual.

  — 6.3 Política de seguridad de la información:

    — REQ-6.3-04X El prestador de servicios de confianza establecerá procedimientos para notificar cualquier modificación en la prestación del servicio de confianza al organismo de supervisión, de conformidad con los requisitos empresariales y las disposiciones legales y reglamentarias pertinentes. El prestador de servicios de confianza notificará al organismo de supervisión competente, como mínimo:

      — cualquier modificación un mes antes de llevarla a cabo;

      — el cese previsto de la prestación de un servicio de confianza tres meses antes de que se produzca.

  — 7.2 Recursos humanos:

    — REQ-7.2-04X El personal del prestador de servicios de confianza en funciones de confianza deberá ser capaz de cumplir el requisito de poseer «los conocimientos especializados, la experiencia y las cualificaciones necesarios» obtenidos a través de formación y credenciales formales, o de la experiencia real, o de una combinación de ambas cosas.

— REQ-7.2-05X Esto incluirá actualizaciones periódicas (al menos cada doce meses) sobre las nuevas amenazas y las prácticas de seguridad actuales.

— 7.5 Controles criptográficos:

— REQ-7.5-01X Se establecerán controles de seguridad adecuados para la gestión de las claves criptográficas, los algoritmos criptográficos y los dispositivos criptográficos a lo largo de todo su ciclo de vida, siguiendo, cuando proceda, un enfoque de agilidad criptográfica.

— REQ-7.5-02 A efectos de la prestación de sus servicios de confianza, el prestador de servicios de confianza seleccionará y utilizará técnicas criptográficas adecuadas conformes con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por ENISA [1].

En particular:

— REQ-7.5-03 Los prestadores de libros mayores electrónicos cualificados establecerán el origen de los registros de datos en el libro mayor electrónico. A tal fin, utilizarán firmas electrónicas avanzadas basadas en certificados cualificados o sellos electrónicos avanzados basados en certificados cualificados creados por los usuarios del servicio de conformidad con las siguientes normas y especificaciones:

a) ETSI EN 319 122-1 V1.3.1 (2023-06), firmas electrónicas e infraestructuras (ESI); firmas digitales CAdES; Parte 1: Componentes elementales y firmas básicas CAdES.

b) ETSI EN 319 132-1 V1.3.1 (2024-07), Electronic Signatures and Trust Infrastructures (ESI) [«Firmas electrónicas e infraestructuras de confianza (ESI)»]; firmas digitales XAdES; Parte 1: Componentes elementales y firmas básicas XAdES.

c) ETSI TS 119 182-1 V1.2.1 (2024-07). Electronic Signatures and Trust Infrastructures (ESI) [«Firmas electrónicas e infraestructuras de confianza (ESI)»]; firmas digitales JAdES; Parte 1: Componentes elementales y firmas básicas JAdES, con la siguiente adaptación:

— 5.1.8 El parámetro del encabezamiento x5c (Cadena de certificados X.509)

— El parámetro del encabezamiento x5c, tal como se define en la cláusula 4.1.6 del documento IETF RFC 7515 [2], estará presente en la firma JAdES, como parámetro del encabezamiento, firmado o no firmado.

— El parámetro del encabezamiento x5c tendrá la semántica especificada en IETF RFC 7515 [2], cláusula 4.1.6.

— El parámetro del encabezamiento x5c tendrá la sintaxis especificada en IETF RFC 7515 [2], cláusula 4.1.6.

— REQ-7.5-04: Los prestadores de libros mayores electrónicos cualificados garantizarán la unicidad del orden cronológico secuencial de los registros de datos en el libro mayor electrónico. Para ello, utilizarán vínculos criptográficos, basados en listas o árboles *hash*, utilizando funciones *hash* criptográficas, de conformidad con las especificaciones y normas siguientes:

a) SHA de 256 bits o superior, de conformidad con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por ENISA [1].

b) SHA3 de 256 bits o superior, de conformidad con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por ENISA [1].

Como alternativa, al utilizar el registro del tiempo para garantizar la unicidad del orden cronológico secuencial de los registros de datos en el libro mayor electrónico, los prestadores de libros mayores electrónicos cualificados utilizarán sellos de tiempo cualificados.

— REQ-7.5-05 Los prestadores de libros mayores electrónicos cualificados garantizarán la integridad de los registros de datos en el libro mayor electrónico cualificado. A tal fin, utilizarán firmas electrónicas avanzadas basadas en certificados cualificados o sellos electrónicos avanzados basados en certificados cualificados, de conformidad con las siguientes normas y especificaciones:

a) Cualquier formato de firma o sello que sea conforme con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por ENISA [1].

b) SHA de 256 bits o superior, de conformidad con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por ENISA [1].

c) SHA3 de 256 bits o superior, de conformidad con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por ENISA [1].

d) Los prestadores de libros mayores electrónicos cualificados garantizarán la detectabilidad inmediata de cualquier modificación posterior de los datos registrados en el libro mayor electrónico.

— REQ-7.5-06 Cuando se utilicen mecanismos de firma digital, se conservarán y utilizarán claves privadas de firma del prestador del libro mayor electrónico cualificado dentro de un dispositivo criptográfico seguro que sea un sistema fiable certificado de conformidad con:

a) los criterios comunes para la evaluación de la seguridad de las tecnologías de la información, tal como se establecen en la norma ISO/IEC 15408 ([1]) [6] o en los criterios comunes para la evaluación de la seguridad de las tecnologías de la información, versión CC:2022, partes 1 a 5, publicados por los participantes en el Acuerdo sobre el reconocimiento de certificados de criterios comunes en el ámbito de la seguridad informática, y con certificación EAL 4 o superior; o

b) el esquema europeo de certificación de la ciberseguridad basado en los criterios comunes (EUCC) ([2]) ([3]) [4] [5] y con certificación EAL 4 o superior; o

c) hasta el 31.12.2030, FIPS PUB 140-3 ([4]) [3] nivel 3.

Esta certificación se referirá a un objetivo de seguridad o perfil de protección, o a una documentación sobre seguridad y diseño de módulo, que cumpla los requisitos del presente documento, sobre la base de un análisis de riesgos y teniendo en cuenta las medidas de seguridad físicas y otras medidas de seguridad no técnicas.

Si el dispositivo criptográfico seguro cuenta con una certificación EUCC [4][5], dicho dispositivo se configurará y utilizará de conformidad con dicha certificación.

([1]) ISO/IEC 15408:2022 (partes 1 a 5): «Seguridad de la información, ciberseguridad y protección de la privacidad. Criterios de evaluación para la seguridad de TI».

([2]) Reglamento de Ejecución (UE) 2024/482 de la Comisión, de 31 de enero de 2024, por el que se establecen disposiciones de aplicación del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo en lo concerniente a la adopción del esquema europeo de certificación de la ciberseguridad basado en los criterios comunes (EUCC), (DO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/2025-01-08).

([3]) Reglamento de Ejecución (UE) 2024/3144 de la Comisión, de 18 de diciembre de 2024, por el que se modifica el Reglamento de Ejecución (UE) 2024/482 en lo que respecta a las normas internacionales aplicables y se corrige dicho Reglamento de Ejecución (DO 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 seguridad para módulos criptográficos»).

— 7.8 Seguridad de la red:

— REQ-7.8-14X El escaneado de vulnerabilidades exigido en el REQ-7.8-13 se realizará al menos una vez al trimestre.

— REQ-7.8-18X La prueba de penetración exigida en el REQ-7.8-17X se realizará al menos una vez al año.

— REQ-7.8-21X: Los cortafuegos también estarán configurados de manera que impidan todos los protocolos y accesos que no sean necesarios para el funcionamiento del prestador de servicios de confianza.

— 7.9.1. Seguimiento y registro:

— REQ-7.9.1-02X Las actividades de seguimiento tendrán en cuenta la sensibilidad de cualquier información recogida o analizada.

— 7.12 Cese y planes de cese del prestador de servicios de confianza:

— REQ-7.12-02A El plan de cese del prestador de servicios de confianza cumplirá los requisitos establecidos en los actos de ejecución adoptados en virtud del artículo 24, apartado 5, del Reglamento (UE) n.º 910/2014 [i.1].

b) Además, para todos los prestadores de libros mayores electrónicos cualificados que utilicen tecnologías de libros mayores electrónicos distribuidos:

1) ISO 23257:2022 Tecnologías de cadena de bloques y de libros mayores distribuidos. Arquitectura de referencia, cláusula 9, que proporciona una descripción completa del sistema tecnológico de libro mayor electrónico distribuido, la red tecnológica de libro mayor electrónico distribuido correspondiente y los nodos tecnológicos de libro mayor electrónico distribuido.

2) ISO/TS 23635:2022. Tecnologías de cadena de bloques y libros mayores distribuidos — Directrices para la gobernanza, con respecto a las políticas y prácticas disponibles por escrito y accesibles al público relacionadas con la estructura de gobernanza del servicio de libro mayor electrónico que prestan.