Diario Oficial
de la Unión Europea

ES
Serie L

2025/1929

30.9.2025

REGLAMENTO DE EJECUCIÓN (UE) 2025/1929 DE LA COMISIÓN

de 29 de septiembre 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 la vinculación de la fecha y la hora con los datos y al establecimiento de la exactitud de las fuentes de información temporal para el suministro de sellos cualificados de tiempo electrónicos

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 42, apartado 2,

Considerando lo siguiente:

(1) Los sellos cualificados de tiempo electrónicos desempeñan un papel crucial en el entorno digital al promover la transición de los procesos tradicionales en papel a procedimientos electrónicos equivalentes. Al vincular la fecha y la hora con los datos electrónicos, los sellos cualificados de tiempo electrónicos ayudan a garantizar la exactitud de la fecha y la hora que indican y la integridad de los documentos digitales a los que están vinculadas la fecha y la hora.

(2) La presunción de cumplimiento establecida en el artículo 42, apartado 1 *bis*, del Reglamento (UE) n.º 910/2014 solo debe aplicarse cuando los servicios de confianza cualificados para la expedición de sellos cualificados de tiempo cumplan las normas establecidas en el presente Reglamento. Estas normas deben reflejar las prácticas establecidas y ser ampliamente aceptadas en los sectores pertinentes. Estas normas deben adaptarse para incluir controles adicionales que garanticen la seguridad y la fiabilidad del servicio de confianza cualificado y de la vinculación de la fecha y la hora con los datos, así como la exactitud de la fuente de información temporal.

(3) 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.

(4) La Comisión evalúa periódicamente las nuevas tecnologías, prácticas, normas y especificaciones técnicas. De conformidad con el considerando 75 del Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo ([2]), la Comisión debe revisar y actualizar el presente Reglamento de Ejecución, en caso necesario, para mantenerlo en consonancia con la evolución mundial, las nuevas tecnologías, normas o especificaciones técnicas y seguir las mejores prácticas del mercado interior.

(5) 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.

([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).

([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.

(6) 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 ([5]), emitió su dictamen el 6 de junio de 2025.

(7) 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

Las normas y especificaciones de referencia a que se refiere el artículo 42, apartado 2, del Reglamento (UE) n.º 910/2014 figuran en el anexo del presente Reglamento.

Artículo 2

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 29 de septiembre de 2025.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

([5]) 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).

ANEXO

Lista de normas de referencia y especificaciones para los servicios de sello cualificado de tiempo

Se aplican las normas ETSI EN 319 421 V1.3.1 ([1]) («ETSI EN 319 421») y ETSI EN 319 422 V1.1.1 ([2]) («ETSI EN 319 422») con las adaptaciones siguientes:

1. En el caso de ETSI EN 319 421

   1) 2.1 Referencias normativas

      — [3] 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».

      — [4] ETSI EN 319 401 V3.1.1 (2024-06) «Firmas electrónicas e infraestructuras de confianza (ESI). Requisitos de política general para proveedores de servicios de confianza».

      — [5] ETSI EN 319 422 V1.1.1 (2016-03) Firmas e infraestructuras electrónicas (ESI). Protocolo de sellado de tiempo y perfiles de los dispositivos token de sello de tiempo.

      — [6] sin efecto.

      — [9] 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») ([3]).

      — [10] Reglamento de Ejecución (UE) 2024/482 de la Comisión ([4]), 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).

      — [11] Reglamento de Ejecución (UE) 2024/3144 de la Comisión ([5]), 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.

   2) 3.1 Términos

      — período de validez del certificado: intervalo de tiempo comprendido desde «notBefore» («no antes de») hasta «notAfter» («no después de») inclusive, durante el cual la autoridad de certificación («CA») garantiza que mantendrá información sobre el estado del certificado

   3) 3.3 Siglas

      — EUCC Esquema europeo de certificación de la ciberseguridad basado en los criterios comunes

   4) 6.2 Declaración de prácticas del servicio de confianza

      — OVR-6.2-03 La TSA (autoridad de sellado de tiempo) incluirá declaraciones sobre la disponibilidad de su servicio de sellado de tiempo en su declaración de divulgación.

   5) 7.3 Seguridad del personal

      — OVR-7.3-02 El personal de la TSA en funciones de confianza y, en su caso, sus subcontratistas en funciones de confianza, deberán ser capaces 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.

      — OVR-7.3-03 El cumplimiento de los requisitos de OVR-7.3-02 incluirá actualizaciones periódicas (al menos cada doce meses) sobre las nuevas amenazas y las prácticas de seguridad actuales.

([1]) EN 319 421: Firmas electrónicas e infraestructuras (ESI). Requisitos de política y seguridad para proveedores de servicios de confianza que emiten sellos de tiempo, V1.3.1.
([2]) EN 319 422: Firmas e infraestructuras electrónicas (ESI). Protocolo de sellado de tiempo y perfiles de los dispositivos token de sello de tiempo, V1.1.1 (2016-03), https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf.
([3]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([4]) DO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([5]) DO L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

6) 7.6.2 Generación de claves de la TSU

— TIS-7.6.2-03 La generación de la(s) clave(s) de la TSU (unidad de sellado de tiempo) se llevará a cabo 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 [3] 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) EUCC [10][11] y con certificación EAL 4 o superior; o

c) hasta el 31.12.2030, FIPS PUB 140-3 [7] 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 [10][11], dicho dispositivo se configurará y utilizará de conformidad con dicha certificación.

— TIS-7.6.2-04 sin efecto.

— NOTA 3 sin efecto.

— TIS-7.6.2-05A El algoritmo de generación de claves de la TSU, la longitud de clave de firma resultante y el algoritmo de firma utilizado para firmar sellos de tiempo y certificados de clave pública de la TSU, respectivamente, serán conformes con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad [9] y publicados por ENISA.

— NOTA 4 sin efecto.

— TIS-7.6.2-06 Una clave de firma de TSU solo se exportará e importará a un dispositivo criptográfico seguro diferente cuando dicha exportación e importación se lleven a cabo de forma segura y de conformidad con la certificación de dichos dispositivos.

7) 7.6.3 Protección de la clave privada de la TSU

— TIS-7.6.3-02 La clave privada de la TSU se custodiará y utilizará en 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 [3] o en los criterios comunes para la evaluación de la seguridad de las tecnologías de la información, versión CC:2002, 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) [10] [11] y con certificación EAL 4 o superior; o

c) hasta el 31.12.2030, FIPS PUB 140-3 [7] 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 [10][11], dicho dispositivo se configurará y utilizará de conformidad con dicha certificación.

— TIS-7.6.3-03 sin efecto.

— NOTA 2 sin efecto.

8) 7.6.7 Fin del ciclo de vida de las claves de las TSU

— TIS-7.6.7-03A La fecha de expiración de las claves privadas de las TSU serán conformes con los mecanismos criptográficos acordados [9].

— NOTA 1 sin efecto.

9) 7.10 Seguridad de la red

— OVR-7.10-05 El escaneado de vulnerabilidades exigido en el REQ-7.8-13 de ETSI EN 319 401 [1] se realizará al menos una vez al trimestre.

— OVR-7.10-06 La prueba de penetración exigida por REQ-7.8-17X de ETSI EN 319 401 [1] se realizará al menos una vez al año.

— OVR-7.10-07 Los cortafuegos estarán configurados de manera que impidan todos los protocolos y accesos que no sean necesarios para el funcionamiento de la TSA.

10) 7.14 Cese y planes de cese de la TSA

— OVR-7.14-01A El plan de cese del TSP 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.4].

2. En el caso de ETSI EN 319 422

1) 2.1 Referencias normativas

— [5] sin efecto.

— [6] sin efecto.

— [8] Grupo Europeo de Certificación de la Ciberseguridad, Subgrupo de Criptografía: «Agreed Cryptographic Mechanisms» («Mecanismos criptográficos acordados», documento en inglés).

— [9] RFC 9110 Semántica del HTTP.

2) 4.1.3 Algoritmos *hash* que deben utilizarse

— Se aplicará la siguiente cláusula:

Los algoritmos *hash* utilizados para identificar la información que va a recibir el sello de tiempo, la duración prevista del sello de tiempo y las funciones hash seleccionadas con respecto al tiempo serán conformes con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por ENISA [8].

— NOTA sin efecto.

3) 4.2.3 Algoritmos que deben admitirse

— Se aplicará la siguiente cláusula:

Los algoritmos de firma de los dispositivos token de sello de tiempo que deben admitirse serán conformes con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por ENISA [8].

— NOTA sin efecto.

4) 4.2.4 Longitudes de clave que deben admitirse

— Se aplicará la siguiente cláusula:

Las longitudes de clave del algoritmo de firma para el algoritmo de firma seleccionado serán conformes con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por ENISA.

— NOTA sin efecto.

5) 5.1.3 Algoritmos que deben admitirse

— Se aplicará la siguiente cláusula:

Los algoritmos *hash* para los datos del sello de tiempo que deben admitirse, la duración prevista del sello de tiempo y las funciones hash seleccionadas con respecto al tiempo serán conformes con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por ENISA [8].

— NOTA sin efecto.

6) 5.2.3 Algoritmos que deben utilizarse

— Se aplicará la siguiente cláusula:

Los algoritmos *hash* utilizados para identificar la información que va a recibir el sello de tiempo y los algoritmos de firma de los dispositivos token de sello de tiempo serán conformes con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por ENISA [8].

— NOTA sin efecto.

7) 6.3 Requisitos relativos a las longitudes de clave

— Se aplicará la siguiente cláusula:

La longitud de clave del algoritmo de firma seleccionado del certificado de la TSU será conforme con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por ENISA [8].

— NOTA sin efecto.

8) 6.5 Requisitos relativos a los algoritmos

— Se aplicará la siguiente cláusula:

La clave pública de la TSU y la firma del certificado de esta utilizarán algoritmos que serán conformes con los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por ENISA [8].

— NOTA sin efecto.

9) 7 Perfiles de los protocolos de transporte que deben admitirse

— El cliente y el servidor de sellado de tiempo admitirán el protocolo de sellado de tiempo a través de HTTPS [9], tal como se define en la cláusula 3.4 de IETF RFC 3161 [1].

10) 8 Identificadores de objeto de los algoritmos criptográficos

— Se aplicará la siguiente cláusula:

La clave pública de la TSU y la firma del certificado de esta utilizarán algoritmos de conformidad con lo dispuesto en los mecanismos criptográficos acordados aprobados por el Grupo Europeo de Certificación de la Ciberseguridad y publicados por ENISA [8].

11) 9.1 Declaración de conformidad con el Reglamento

— Si la TSA declara que un testigo de sello de tiempo es un sello cualificado de tiempo electrónico de conformidad con el Reglamento (UE) n.º 910/2014 [i.2], contendrá una instancia de la extensión «qcStatements» en el campo de la extensión del dispositivo token de sello de tiempo con la sintaxis indicada en IETF RFC 3739 [i.3], cláusula 3.2.6.

— La extensión «qcStatements» contendrá una instancia de la declaración «esi4-qtstStatement-1», tal como se define en el anexo B.

— La extensión «qcStatements» no se marcará como crítica.