2025/2160

28.10.2025

REGLAMENTO DE EJECUCIÓN (UE) 2025/2160 DE LA COMISIÓN

de 27 de octubre 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 de referencia, las especificaciones y los procedimientos para la gestión de riesgos para la prestación de servicios de confianza no 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 19 *bis*, apartado 2,

Considerando lo siguiente:

(1) Los prestadores no cualificados de servicios de confianza desempeñan un papel importante en el entorno digital al prestar servicios de confianza que facilitan transacciones electrónicas seguras. El Reglamento (UE) n.º 910/2014 impone menos requisitos reglamentarios a los prestadores no cualificados de servicios de confianza que a los prestadores cualificados de servicios de confianza. Sin embargo, todos los prestadores de servicios de confianza están sujetos a requisitos de seguridad y responsabilidad para garantizar la diligencia debida, la transparencia y la rendición de cuentas de sus operaciones y servicios.

(2) Los prestadores no cualificados de servicios de confianza pueden considerarse entidades importantes o esenciales de conformidad con el artículo 3 de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo ([2]). Así pues, se les aplica el Reglamento de Ejecución (UE) 2024/2690 de la Comisión ([3]), por el que se establecen los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad. Sin embargo, el ámbito de aplicación de los requisitos establecidos en el artículo 19 *bis*, apartado 1, letra a), del Reglamento (UE) n.º 910/2014 se refiere a los procedimientos de gestión de riesgos relativos a los riesgos jurídicos, empresariales, operativos y otros riesgos directos o indirectos para la prestación de servicios de confianza no cualificados. Para complementar el marco de gestión de riesgos establecido en el Reglamento de Ejecución (UE) 2024/2690 y permitir un enfoque coherente de la gestión de todos los tipos de riesgos pertinentes, deben establecerse especificaciones y procedimientos relativos a la gestión de dichos riesgos por parte de prestadores no cualificados de servicios de confianza. Las orientaciones facilitadas por la Agencia de la Unión Europea para la Ciberseguridad (ENISA) o las autoridades nacionales competentes en virtud de la Directiva (UE) 2022/2555 pueden ayudar a los prestadores no cualificados de servicios de confianza en el diseño y la aplicación de políticas adecuadas de gestión de riesgos.

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

([2]) Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) (DO L 333 de 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([3]) Reglamento de Ejecución (UE) 2024/2690 de la Comisión, de 17 de octubre de 2024, por el que se establecen las disposiciones de aplicación de la Directiva (UE) 2022/2555 en lo que respecta a los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad y en el que se detallan los casos en que un incidente se considera significativo con respecto a los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de servicios de computación en nube, los proveedores de servicios de centro de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados, los proveedores de servicios de seguridad gestionados, los proveedores de mercados en línea, motores de búsqueda en línea y plataformas de servicios de redes sociales, y los proveedores de servicios de confianza (DO L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

(3) La presunción de cumplimiento establecida en el artículo 19 *bis*, apartado 2, del Reglamento (UE) n.º 910/2014 solo debe aplicarse cuando los prestadores no cualificados de servicios de confianza cumplan los requisitos establecidos en el presente Reglamento. Las normas de referencia a que se refiere el anexo deben reflejar las prácticas establecidas y ser ampliamente aceptadas en los sectores pertinentes. A fin de garantizar que los prestadores no cualificados de servicios de confianza gestionen los riesgos jurídicos, empresariales, operativos y otros riesgos directos o indirectos para la prestación del servicio de confianza no cualificado de conformidad con el artículo 19 *bis*, apartado 1, del Reglamento (UE) n.º 910/2014, los prestadores no cualificados de servicios de confianza deben cumplir los elementos de referencia de las normas que figuran en el anexo y los requisitos de gestión de riesgos establecidos en el presente Reglamento para la presunción de cumplimiento.

(4) Si un prestador no cualificado de servicios de confianza cumple los requisitos establecidos en el presente Reglamento de Ejecución, los organismos de supervisión deben presumir el cumplimiento de los requisitos pertinentes del Reglamento (UE) n.º 910/2014. No obstante, un prestador no 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) Para garantizar que los riesgos detectados se aborden adecuadamente, las políticas de gestión de riesgos seguidas por los prestadores no cualificados de servicios de confianza deben incluir procedimientos para la documentación y la evaluación de riesgos, así como para la determinación, selección y aplicación de medidas adecuadas de tratamiento del riesgo. La aplicación de medidas de tratamiento de riesgos debe ser objeto de un seguimiento continuo. Por lo que se refiere a la información que los prestadores no cualificados de servicios de confianza registran y conservan como parte de sus medidas de tratamiento del riesgo, los prestadores no cualificados de servicios de confianza deben garantizar la integridad y confidencialidad de dichos datos. Además, para aumentar la transparencia y apoyar las actividades de supervisión, los prestadores no cualificados de servicios de confianza deben publicar los métodos de verificación de la identidad que aplican. Dado que no todos los riesgos detectados pueden abordarse plenamente mediante su evitación, mitigación o transferencia a otras entidades, cualquier riesgo residual debe ser aprobado por los órganos de dirección de los prestadores no cualificados de servicios de confianza. Los criterios para la aceptación de los riesgos residuales deben justificarse de manera comprensible.

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

(7) El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo ([5]) y, en su caso, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo ([6]) son aplicables a las actividades de tratamiento de datos personales en virtud del presente Reglamento.

(8) 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 ([7]), emitió su dictamen el 8 de agosto de 2025 ([8]).

([4]) 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).

([5]) 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).

([6]) 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).

([7]) 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).

([8]) EDPS Formal comments on the draft Implementing Regulation as regards specifications and procedures for the management of risks to the provision of non-qualified trust services | European Data Protection Supervisor [«Observaciones formales del SEPD sobre el proyecto de Reglamento de Ejecución en lo que respecta a las especificaciones y los procedimientos para la gestión de riesgos para la prestación de servicios de confianza no cualificados | Supervisor Europeo de Protección de Datos», documento en inglés].

(9) 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

Las normas de referencia a que se refiere el artículo 19 *bis*, apartado 2, del Reglamento (UE) n.º 910/2014 figuran en el anexo del presente Reglamento.

Artículo 2

Políticas de gestión de riesgos

1. Las políticas de gestión de riesgos a que se refiere el artículo 19 *bis*, apartado 1, del Reglamento (UE) n.º 910/2014 identificarán claramente los servicios de confianza a los que se aplican, serán específicas de los servicios de confianza de que se trate y serán aprobadas por el órgano de dirección del prestador no cualificado de servicios de confianza.

2. Las políticas de gestión de riesgos incluirán al menos los elementos siguientes:

a) el nivel global de tolerancia al riesgo de acuerdo con el carácter crítico y el nivel de seguridad requerido de los servicios de confianza, teniendo en cuenta los últimos avances tecnológicos;

b) los criterios de riesgo pertinentes, incluidos, como mínimo, la probabilidad, el impacto y el nivel del riesgo, teniendo en cuenta la inteligencia sobre ciberamenazas y las vulnerabilidades;

c) un enfoque para la detección y documentación de los riesgos para la prestación de los servicios de confianza, teniendo en cuenta el alcance completo del sistema de información utilizado por el prestador no cualificado de servicios de confianza, incluidos los riesgos asociados a los componentes del sistema, así como a cualquier parte activa o pasiva que participe en la aplicación del sistema o en la prestación de los servicios de confianza;

d) un proceso para la evaluación de los riesgos detectados sobre la base de los criterios de riesgo a que se refiere la letra b);

e) un proceso para la determinación, priorización y seguimiento continuo de la aplicación de medidas adecuadas de tratamiento del riesgo;

f) un proceso de seguimiento continuo de la aplicación de las políticas de gestión de riesgos.

3. Los prestadores no cualificados de servicios de confianza establecerán procedimientos adecuados y conservarán documentos para garantizar la aplicación de los requisitos establecidos en la legislación aplicable.

4. Los prestadores no cualificados de servicios de confianza establecerán procedimientos documentados adecuados que garanticen el seguimiento de los cambios legislativos y reglamentarios nacionales y de la Unión que puedan afectar a la prestación de servicios de confianza.

Artículo 3

Detección, documentación y evaluación de riesgos

Los prestadores no cualificados de servicios de confianza detectarán, documentarán y evaluarán todos los riesgos a que se refiere el artículo 19 *bis*, apartado 1, del Reglamento (UE) n.º 910/2014, de conformidad con las políticas de gestión de riesgos a que se refiere el artículo 2, y en particular:

a) detectarán los riesgos en relación con terceros;

b) determinarán un posible punto único de fallo en la prestación de los servicios de confianza;

c) evaluarán los riesgos detectados sobre la base de los criterios de riesgo a que se refiere el artículo 2, apartado 2, letra b).

Artículo 4

Medidas de tratamiento de riesgos

1. De conformidad con las políticas a que se refiere el artículo 2, los prestadores no cualificados de servicios de confianza planificarán, documentarán y aplicarán medidas de tratamiento de riesgos y, en particular, llevarán a cabo las siguientes tareas:

a) determinarán y priorizarán las medidas adecuadas de tratamiento de riesgos;

b) seleccionarán, aprobarán y documentarán las medidas de tratamiento del riesgo elegidas, incluidos sus requisitos de seguridad y procedimientos operativos, en un plan de tratamiento de riesgos, determinarán quién es responsable de la aplicación de las medidas de tratamiento del riesgo y cuándo deben aplicarse;

c) supervisarán constantemente la aplicación de las medidas de tratamiento de riesgos.

2. El plan de tratamiento de riesgos establecido en el apartado 1, letra b), expondrá las razones que justifiquen la aceptación de los riesgos residuales de manera comprensible.

3. Como parte de las medidas de tratamiento de riesgos a que se refiere el apartado 1, los prestadores no cualificados de servicios de confianza:

a) verificarán, cuando proceda, la identidad de los usuarios del servicio de confianza directamente o por medio de un tercero y publicarán información sobre los métodos de verificación de la identidad utilizados;

b) a efectos de aportar pruebas en procedimientos judiciales y de garantizar la continuidad del servicio, registrarán y conservarán de forma segura durante el tiempo que sea necesario de conformidad con el Derecho de la Unión o nacional, incluso después de que hayan cesado las actividades del prestador no cualificado de servicios de confianza, la siguiente información:

— toda la información pertinente recogida en el proceso de registro e incorporación de los usuarios de servicios de confianza, incluida, en su caso, la verificación de la identidad de los usuarios,

— los datos de autenticación asignados al usuario del servicio de confianza, cuando proceda, y

— cualquier cambio en el estado de los certificados de clave pública u otro material criptográfico utilizado en la prestación del servicio de confianza.

c) garantizarán, cuando proceda, que los datos de autenticación asignados al usuario del servicio de confianza sean únicos.

4. Al determinar, seleccionar, aprobar y priorizar medidas adecuadas de tratamiento del riesgo, los prestadores no cualificados de servicios de confianza tendrán en cuenta los siguientes elementos:

a) los resultados de la evaluación de riesgos a que se refiere el artículo 3;

b) la efectividad de las medidas de tratamiento de riesgos;

c) la evaluación de la conformidad;

d) los incidentes significativos;

e) el coste de la implementación en relación con el beneficio previsto;

f) la clasificación de activos apropiada aplicable;

g) el análisis de cualquier impacto económico de los riesgos detectados de conformidad con el artículo 3.

5. Los órganos de dirección de los prestadores no cualificados de servicios de confianza aprobarán los riesgos residuales restantes tras la aplicación de las medidas de tratamiento de riesgos establecidas en el plan de tratamiento de riesgos.

6. Los prestadores no cualificados de servicios de confianza revisarán, documentarán y, cuando proceda, actualizarán los resultados de la evaluación de riesgos y el plan de tratamiento de riesgos a intervalos planificados, y al menos una vez al año, y cuando se produzcan cambios significativos en la infraestructura, las operaciones o los riesgos, o incidentes significativos.

7. Los prestadores no cualificados de servicios de confianza garantizarán la disponibilidad, integridad y confidencialidad de la información a que se refiere el apartado 3, letra b).

Artículo 5

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 27 de octubre de 2025.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

ANEXO

Lista de normas de referencia para prestadores no cualificados de servicios de confianza

Se aplicarán los requisitos de las siguientes cláusulas de la norma ETSI EN 319 401 V3.1.1 (2024-06): «Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers» [«Firmas electrónicas e infraestructuras de confianza (ESI). Requisitos de política general para proveedores de servicios de confianza», documento en inglés]:

5. Evaluación de riesgos.

6. Políticas y prácticas.

7.1 Organización interna.

7.2 Recursos humanos.

7.3 Gestión de activos.

7.4 Control de acceso.

7.6 Seguridad física y del entorno.