2024/3144

19.12.2024

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 relativo a las normas internacionales aplicables y se corrige dicho Reglamento de Ejecución

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad») ([1]), y en particular su artículo 49, apartado 7,

Considerando lo siguiente:

(1) El Reglamento de Ejecución (UE) 2024/482 de la Comisión ([2]) especifica las funciones, normas y obligaciones, así como la estructura del esquema europeo de certificación de la ciberseguridad basado en los criterios comunes (en lo sucesivo, «EUCC»), de conformidad con el marco europeo de certificación de la ciberseguridad establecido en el Reglamento (UE) 2019/881.

(2) El Reglamento de Ejecución (UE) 2024/482 se basa en normas internacionales establecidas que son los criterios comunes y la metodología común de evaluación mantenidos por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (CEI o IEC, por sus siglas en inglés). El Reglamento de Ejecución (UE) 2024/482 hace referencia a las normas ISO/IEC, pero no especifica la versión aplicable de dichas normas. Por lo tanto, debe especificarse qué versión de las normas se aplica a los certificados expedidos en virtud del EUCC.

(3) Las organizaciones gubernamentales que contribuyeron a la elaboración de los criterios comunes y la metodología común de evaluación a través del Acuerdo de reconocimiento de los criterios comunes (CCRA), que garantiza el reconocimiento de los certificados de criterios comunes en el ámbito de la seguridad informática, son cotitulares, junto con la ISO/IEC, de los derechos de autor sobre ellos. Estas organizaciones gubernamentales conservan el derecho a utilizarlas. Habida cuenta de la importancia de estos documentos procedentes del CCRA, también deberían sentar las bases para la certificación en virtud del EUCC.

(4) Las normas relativas a los criterios comunes y a la metodología común de evaluación están sujetas a interpretaciones por parte del CCRA que facilitan su aplicación y que las instalaciones de evaluación de la seguridad de las tecnologías de la información (ITSEF) y los organismos de certificación pueden tener en cuenta.

(5) Las normas internacionales relacionadas con los criterios comunes podrían ser objeto de actualizaciones. A fin de garantizar una transición ordenada y oportuna, conviene definir unas normas de transición para que los proveedores, las ITSEF y los organismos de certificación, así como otros agentes pertinentes, dispongan del tiempo suficiente para realizar los ajustes necesarios. Dichas normas de transición deben adaptarse, en la medida adecuada, a las prácticas mundiales, como las establecidas por el CCRA.

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

([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/oj).

(6) El Reglamento de Ejecución (UE) 2024/482 no especifica hasta cuándo la certificación de un producto de TIC podría basarse en las versiones anteriores de las normas relativas a los criterios comunes y a la metodología común de evaluación. Los ámbitos técnicos y los perfiles de protección enumerados en los anexos I, II y III de dicho Reglamento de Ejecución se basan en versiones anteriores de las normas ISO/IEC 15408 y 18045. Por consiguiente, el Reglamento de Ejecución (UE) 2024/482 debe especificar en qué circunstancias se seguirá aplicando la versión anterior de los criterios comunes y de la metodología común de evaluación y cómo funcionará la transición a la última versión de las normas internacionales.

(7) Durante el período de transición, debe ser prioritario que las partes interesadas pertinentes actualicen los ámbitos técnicos y los perfiles de protección correspondientes. El Reglamento de Ejecución (UE) 2024/482 debe disponer que los objetivos de seguridad basados en una versión anterior de las normas se acepten hasta el 31 de diciembre de 2027, en consonancia con la política de transición adoptada por el CCRA. Sin embargo, cabe señalar que la política de transición del CCRA contempla las evaluaciones iniciales de los productos y perfiles de protección que comienzan, a más tardar, el 30 de junio de 2024, fecha en la que todavía no se aplicaba el EUCC. Además, en consonancia con la política de transición del CCRA, el Reglamento de Ejecución (UE) 2024/482 debe disponer que los objetivos de seguridad conformes con dicho Reglamento de Ejecución y declarados conformes con los perfiles de protección basados en una versión anterior de las normas se acepten hasta el 31 de diciembre de 2027. Asimismo, cuando se expida un nuevo certificado en virtud del Reglamento de Ejecución (UE) 2024/482 en el marco de un proceso de revisión de un certificado nacional que comience en un plazo de dos años a partir del certificado inicial, debe ser posible utilizar una versión anterior de las normas. Esto no afectaría a un proceso de revisión que no requiera la expedición de un nuevo certificado con arreglo al Reglamento de Ejecución (UE) 2024/482 y en el que el certificado siga siendo válido.

(8) A fin de garantizar una transición ordenada a la versión más reciente de las normas, el Reglamento de Ejecución (UE) 2024/482 debe establecer normas transitorias específicas y seguir permitiendo la expedición de certificados en virtud de dicho Reglamento de Ejecución declarados conformes con los perfiles de protección basados en versiones anteriores de las normas publicadas por el CCRA cuando la legislación de la Unión exija el uso de dichos perfiles de protección. Este es el caso del Reglamento de Ejecución (UE) 2016/799 de la Comisión ([3]), del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo ([4]) y de la Decisión de Ejecución (UE) 2016/650 de la Comisión ([5]).

(9) En el anexo I del Reglamento de Ejecución (UE) 2024/482 se enumeran los documentos del estado de la técnica aplicables a la evaluación de los productos de TIC y los perfiles de protección. Sin embargo, no especifica la versión de los documentos. Por lo tanto, debe especificarse qué versión de los documentos se aplica a los certificados expedidos en virtud del EUCC. Dichas versiones se basan en documentos aprobados por el Grupo Europeo de Certificación de la Ciberseguridad (GECC) y fueron sometidas una revisión adicional para ser incluidas en el EUCC. Además, debe modificarse el anexo I para incluir documentos del estado de la técnica nuevos y actualizados tras ser aprobados por el GECC, garantizando así una acreditación uniforme de los organismos de evaluación de la conformidad en el marco del EUCC. Los requisitos relativos a la acreditación de las ITSEF deben actualizarse para aclarar la aplicación de los criterios de independencia e imparcialidad, y debe elaborarse un nuevo documento del estado de la técnica para la acreditación de los organismos de certificación.

(10) Los documentos del estado de la técnica podrían añadirse al EUCC o podrían ser objeto de actualizaciones en el contexto de las actividades de mantenimiento. En el caso de los documentos del estado de la técnica nuevos o actualizados, podría ser necesario establecer normas de transición adecuadas que permitan que los vendedores, las ITSEF, los organismos de certificación y otras partes interesadas realicen los ajustes necesarios. En cuanto a la actualización del documento del estado de la técnica relativo a la acreditación de las ITSEF, el documento actualizado debe aplicarse a las acreditaciones expedidas antes del 8 de julio de 2025 únicamente cuando sean objeto de una revisión, por ejemplo en el contexto de un procedimiento de evaluación o reevaluación. Además, el documento actualizado debe aplicarse a todas las acreditaciones de las ITSEF expedidas después del 8 de julio de 2025.

([3]) Reglamento de Ejecución (UE) 2016/799 de la Comisión, de 18 de marzo de 2016, por el que se ejecuta el Reglamento (UE) n.º 165/2014 del Parlamento Europeo y del Consejo, que establece los requisitos para la construcción, ensayo, instalación, funcionamiento y reparación de los tacógrafos y de sus componentes (DO L 139 de 26.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

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

([5]) Decisión de Ejecución (UE) 2016/650 de la Comisión, de 25 de abril de 2016, por la que se fijan las normas para la evaluación de la seguridad de los dispositivos cualificados de creación de firmas y sellos con arreglo al artículo 30, apartado 3, y al artículo 39, apartado 2, del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (DO L 109 de 26.4.2016, p. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).

(11) Realizar correcciones complementarias de los artículos 5, 8, 16, 29 y 44, y al anexo IV del Reglamento de Ejecución (UE) 2024/482 ayuda a garantizar una redacción uniforme y una interpretación jurídica clara.

(12) Las normas relativas a las notificaciones de los organismos de evaluación de la conformidad deben establecerse horizontalmente para todos los esquemas en el marco europeo de certificación de la ciberseguridad. Las normas relativas a dichas notificaciones se contemplan en el Reglamento de Ejecución (UE) 2024/3143 ([6]). Así pues, los artículos 23 y 24 del Reglamento de Ejecución (UE) 2024/482 deben suprimirse a partir de la fecha de aplicación del Reglamento de Ejecución (UE) 2024/3143.

(13) Procede, por tanto, modificar y corregir el Reglamento de Ejecución (UE) 2024/482 en consecuencia.

(14) Las medidas previstas en el presente Reglamento se ajustan al dictamen del Comité creado en virtud del artículo 66 del Reglamento (UE) 2019/881.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

El Reglamento de Ejecución (UE) 2024/482 se modifica como sigue:

1) En el artículo 2, los puntos 1) y 2) se sustituyen por el texto siguiente:

«1) "criterios comunes": los criterios comunes para la evaluación de la seguridad de las tecnologías de la información, tal como se establecen en las normas ISO/IEC 15408-1:2022, ISO/IEC 15408-2:2022, ISO/IEC 15408-3:2022, ISO/IEC 15408-4:2022 o ISO/IEC 15408-5:2022, o bien 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;

2) "metodología común de evaluación": la metodología común para la evaluación de la seguridad de las tecnologías de la información, tal como se establece en la norma ISO/IEC 18045:2022, o la metodología común para la evaluación de la seguridad de las tecnologías de la información, versión CEM:2022, publicada por los participantes en el Acuerdo sobre el reconocimiento de certificados de criterios comunes en el ámbito de la seguridad informática;».

2) El artículo 3 se sustituye por el texto siguiente:

«*Artículo 3*

Normas de evaluación

1. Las evaluaciones efectuadas en el marco del esquema EUCC se regirán por las siguientes normas:

a) los criterios comunes;

b) la metodología común de evaluación.

2. Hasta el 31 de diciembre de 2027, podrá expedirse un certificado con arreglo al esquema EUCC que aplique cualquiera de las siguientes normas:

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

b) los criterios comunes para la evaluación de la seguridad de las tecnologías de la información, versión 3.1, revisión 5, publicados por los participantes en el Acuerdo sobre el reconocimiento de certificados de criterios comunes en el ámbito de la seguridad informática;

([6]) Reglamento de Ejecución (UE) 2024/3143 de la Comisión, de 18 de diciembre de 2024, por el que se establecen las circunstancias, los formatos y los procedimientos de notificación con arreglo al artículo 61, apartado 5, del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación (DO L, 2024/3143, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3143/oj).

c) ISO/IEC 18045:2008;

d) la metodología común para la evaluación de la seguridad de las tecnologías de la información, revisión 5, versión 3.1, publicada por los participantes en el Acuerdo sobre el reconocimiento de certificados de criterios comunes en el ámbito de la seguridad informática;

3. Hasta el 31 de diciembre de 2027, podrá expedirse un certificado que aplique las normas a que se refiere el apartado 1 en el marco del esquema EUCC declarado conforme con un perfil de protección que haya aplicado las normas enumeradas en el apartado 2.

4. También podrá expedirse en el marco del esquema EUCC un certificado que aplique las normas a que se refiere el apartado 1 declarado conforme con un perfil de protección que haya aplicado cualquiera de las siguientes normas, siempre que el uso de dicho perfil de protección sea obligatorio en virtud del Reglamento de Ejecución (UE) 2016/799 de la Comisión (*), el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo (**)o la Decisión de Ejecución (UE) 2016/650 de la Comisión (***):

a) los criterios comunes para la evaluación de la seguridad de las tecnologías de la información, versión 3.1, revisiones 1 a 4, publicados por los participantes en el Acuerdo sobre el reconocimiento de certificados de criterios comunes en el ámbito de la seguridad informática;

b) la metodología común para la evaluación de la seguridad de las tecnologías de la información, versión 3.1, revisiones 1 a 4, publicada por los participantes en el Acuerdo sobre el reconocimiento de certificados de criterios comunes en el ámbito de la seguridad informática;

_____

(*) Reglamento de Ejecución (UE) 2016/799 de la Comisión, de 18 de marzo de 2016, por el que se ejecuta el Reglamento (UE) n.º 165/2014 del Parlamento Europeo y del Consejo, que establece los requisitos para la construcción, ensayo, instalación, funcionamiento y reparación de los tacógrafos y de sus componentes (DO L 139 de 26.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

(**) 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 la que se deroga la Directiva 1999/93/CE (DO L 257 de 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

(***) Decisión de Ejecución (UE) 2016/650 de la Comisión, de 25 de abril de 2016, por la que se fijan las normas para la evaluación de la seguridad de los dispositivos cualificados de creación de firmas y sellos con arreglo al artículo 30, apartado 3, y al artículo 39, apartado 2, del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (DO L 109 de 26.4.2016, p. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).».

3) En el capítulo IV, se inserta el artículo 20 *bis* siguiente:

«*Artículo 20* bis

Especificación de los requisitos para la acreditación de los organismos de evaluación de la conformidad

La acreditación de los organismos de evaluación de la conformidad tendrá en cuenta la especificación de los requisitos relativos a la acreditación de los organismos de certificación y las ITSEF, establecidos en los documentos del estado de la técnica aplicables enumerados en el punto 2 del anexo I.».

4) Se suprimen los artículos 23 y 24.

5) En el artículo 48 se añade el apartado 4 siguiente:

«4. Salvo disposición en contrario en los anexos I o II, los documentos del estado de la técnica se aplicarán a partir de la fecha de aplicación del acto modificativo por el que fueron incorporados a los anexos I o II.».

6) En el artículo 49 se añade el apartado 4 siguiente:

«4. Al llevar a cabo la revisión a que se refiere el apartado 3 en un plazo de dos años a partir de la expedición del certificado inicial, y cuando dicha revisión dé lugar a la expedición de un nuevo certificado de conformidad con el presente Reglamento, podrán aplicarse las normas enumeradas en el artículo 3, apartado 2. La fecha de expedición del certificado inicial se entenderá como la fecha de expedición del último certificado para un producto de TIC o perfil de protección en el que se basa la certificación actual.».

7) El anexo I se sustituye por el texto que figura en el anexo I del presente Reglamento.

8) El anexo IV se modifica de conformidad con el anexo II del presente Reglamento.

Artículo 2

El Reglamento de Ejecución (UE) 2024/482 se corrige como sigue:

1) En el artículo 5, apartado 1, la letra b) se sustituye por el texto siguiente:

«b) declarando la conformidad con un perfil de protección certificado en el marco del proceso de TIC, cuando el producto de TIC pertenezca a la categoría de productos de TIC cubierta por dicho perfil de protección.».

2) El artículo 8 se corrige como sigue:

a) el título se sustituye por el texto siguiente:

«Información necesaria para la certificación y la evaluación»;

b) el apartado 1 se sustituye por el texto siguiente:

«1. El solicitante de una certificación en virtud del EUCC proporcionará al organismo de certificación y a la ITSEF o pondrá a disposición de ambos por otros medios toda la información necesaria para las actividades de certificación y de evaluación.».

3) El artículo 16 se sustituye por el texto siguiente:

«*Artículo 16*

Información necesaria para la certificación y la evaluación de perfiles de protección

El solicitante de la certificación de un perfil de protección proporcionará al organismo de certificación y a la ITSEF, o pondrá a disposición de ambos por otros medios, toda la información necesaria para las actividades de certificación y de evaluación de forma completa y correcta. El artículo 8, apartados 2, 3, 4 y 7, se aplicará *mutatis mutandis*.».

4) En el artículo 17 se suprime el apartado 1.

5) En el artículo 29, el apartado 2 se sustituye por el texto siguiente:

«2. Cuando el titular de un certificado EUCC no proponga medidas correctoras adecuadas durante el plazo a que se refiere el apartado 1, se procederá a suspender el certificado de conformidad con el artículo 30 o a retirarlo de conformidad con el artículo 14 o el artículo 20.».

Artículo 3

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

El artículo 1, apartado 4, será aplicable a partir del 8 de enero de 2025.

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

Hecho en Bruselas, el 18 de diciembre de 2024.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

ANEXO I

«ANEXO I

Documentos del estado de la técnica en apoyo de los ámbitos técnicos y otros documentos del estado de la técnica

1. Documentos del estado de la técnica en apoyo de los ámbitos técnicos en los niveles AVA_VAN 4 o 5:

   a) los siguientes documentos relacionados con la evaluación armonizada del ámbito técnico "tarjetas inteligentes y dispositivos similares" [disponibles en inglés]:

      1) Minimum ITSEF requirements for security evaluations of smart cards and similar devices ["Requisitos mínimos aplicables a las ITSEF para las evaluaciones de seguridad de tarjetas inteligentes y dispositivos similares"], versión 1.1;

      2) Minimum Site Security Requirements ["Requisitos mínimos de seguridad de las instalaciones"], versión 1.1;

      3) Application of Common Criteria to integrated circuits ["Aplicación de los criterios comunes a los circuitos integrados"], versión 1.1;

      4) Security Architecture requirements (ADV_ARC) for smart cards and similar devices ["Requisitos de arquitectura de seguridad (ADV_ARC) para tarjetas inteligentes y dispositivos similares"], versión 1.1;

      5) Certification of "open" smart card products ["Certificación de productos de tarjeta inteligente 'abierta'"], versión 1.1;

      6) Composite product evaluation for smart cards and similar devices ["Evaluación de productos compuestos para tarjetas inteligentes y dispositivos similares"], versión 1.1;

      7) Application of Attack Potential to Smartcards and Similar Devices ["Aplicación de potencial de ataque a tarjetas inteligentes y dispositivos similares"], versión 1.2;

   b) los siguientes documentos relacionados con la evaluación armonizada del ámbito técnico "dispositivos de hardware con cajas de seguridad» [disponibles en inglés]:

      1) Minimum ITSEF requirements for security evaluations of hardware devices with security boxes ["Requisitos mínimos aplicables a las ITSEF para las evaluaciones de seguridad de dispositivos de hardware con cajas de seguridad"], versión 1.1;

      2) Minimum Site Security Requirements ["Requisitos mínimos de seguridad de las instalaciones"], versión 1.1;

      3) Application of Attack Potential to Hardware Devices with Security Boxes ["Aplicación de potencial de ataque a dispositivos de hardware con cajas de seguridad"], versión 1.2;

2. Documentos del estado de la técnica relativos a la acreditación armonizada de los organismos de evaluación de la conformidad [disponibles en inglés]:

   a) Accreditation of ITSEFs for the EUCC ["Acreditación de ITSEF a efectos del EUCC"], versión 1.1, para las acreditaciones expedidas antes del 8 de julio de 2025.

   b) Accreditation of ITSEFs for the EUCC ["Acreditación de ITSEF a efectos del EUCC"], versión 1.6c, para las acreditaciones expedidas recientemente o revisadas después del 8 de julio de 2025.

   c) Accreditation of CBs for the EUCC ["Acreditación de organismos de certificación para el EUCC"], versión 1.6b.».

ANEXO II

En el anexo IV del Reglamento de Ejecución (UE) 2024/482, sección IV.3, los puntos 5 y 6 se sustituyen por el texto siguiente:

«5. Cuando el organismo de certificación haya confirmado que las modificaciones son menores, no se expedirá un nuevo certificado para el producto de TIC modificado y se elaborará un informe de mantenimiento del informe de certificación inicial.

El informe de mantenimiento se incluirá como subconjunto del informe de evaluación de impacto y contendrá las siguientes secciones:

a) introducción;

b) descripción de las modificaciones;

c) pruebas aportadas por el desarrollador afectado.

6. El informe de mantenimiento a que se refiere el apartado 5 se transmitirá a ENISA para que lo publique en su sitio web de certificación de la ciberseguridad.».