Diario Oficial
de la Unión Europea

ES
Serie L

2025/2462

9.12.2025

REGLAMENTO DE EJECUCIÓN (UE) 2025/2462 DE LA COMISIÓN

de 8 de diciembre de 2025

por el que se modifica el Reglamento de Ejecución (UE) 2024/482 en lo que respecta a las definiciones, la certificación de las series de productos de TIC, la continuidad de la garantía y los documentos del estado de la técnica

(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) La metodología común de evaluación que acompaña a los criterios comunes, una norma internacional para la evaluación de la seguridad de las tecnologías de la información, permite evaluar la seguridad de los productos de TIC a efectos de certificación. En este contexto, algunos productos de TIC pueden utilizar la misma base funcional para ofrecer funcionalidades de seguridad similares en diferentes plataformas o dispositivos, lo que también se denomina «serie de productos». Sin embargo, el diseño, el *hardware*, el *firmware* o el programa informático pueden variar de un producto de TIC a otro. Corresponde al organismo de certificación decidir caso por caso si puede llevarse a cabo la certificación de una serie de productos. Las condiciones para la certificación de series de productos podrían explicarse más detalladamente en unas directrices de apoyo del EUCC.

(3) A fin de mantener la fiabilidad de los productos certificados, es fundamental definir qué constituye una modificación importante y menor en el objeto de evaluación o su entorno, en particular sus entornos operativos o de desarrollo. Es, pues, necesario precisar dichos conceptos teniendo en cuenta las especificaciones técnicas existentes y ampliamente utilizadas del Grupo de altos funcionarios sobre seguridad de los sistemas de información (SOG-IS) y de los participantes en el Acuerdo sobre el reconocimiento de certificados de criterios comunes en el ámbito de la seguridad informática (CCRA).

(4) Las modificaciones menores se caracterizan a menudo por su efecto limitado en la declaración de garantía del producto facilitada por el certificado EUCC expedido. Así pues, las modificaciones menores deben gestionarse con arreglo a procedimientos de mantenimiento y no requieren una revaluación de las funcionalidades de seguridad del producto. Entre los ejemplos de modificaciones menores que deben tratarse mediante mantenimiento figuran, entre otros, los cambios de redacción, las modificaciones del entorno del objeto de evaluación que no modifican el objeto de evaluación certificado y las modificaciones en el objeto de evaluación certificado que no afectan a las pruebas de garantía. Las modificaciones en el entorno de desarrollo también pueden considerarse menores, siempre que no tengan un impacto posterior en las medidas de garantía existentes. No obstante, en algunos casos pueden requerir una evaluación parcial de las medidas pertinentes.

([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).

(5) Una modificación importante es cualquier cambio en el objeto de evaluación certificado o en su entorno que puede afectar negativamente a la garantía indicada en el certificado EUCC, por lo que debe requerir una nueva evaluación. Algunos ejemplos de modificaciones importantes son, entre otras, las modificaciones en el conjunto de requisitos de garantía declarados, excepto en el caso de los requisitos de garantía de la familia CC ALC_FLR (corrección de defectos); modificaciones en los controles de confidencialidad o integridad del entorno de desarrollo cuando dichas modificaciones puedan afectar al desarrollo seguro o a la producción del objeto de evaluación o cambios en el objeto de evaluación para resolver una vulnerabilidad aprovechable. Además, un conjunto de modificaciones menores que tienen colectivamente un impacto significativo en la seguridad también puede considerarse una modificación importante. Es también importante reconocer que, si bien una corrección de un fallo puede afectar solamente a un aspecto concreto del objeto de evaluación, su imprevisibilidad y su posible impacto en la garantía pueden convertirla en una modificación importante si compromete las garantías de seguridad proporcionadas por la certificación.

(6) Los cambios producidos en el entorno de amenazas de un producto de TIC certificado que no haya sufrido modificaciones podrían requerir una revaluación. Deben establecerse claramente los posibles resultados de dicho proceso de revaluación, en particular sus repercusiones en el certificado EUCC. Si se completa con éxito una revaluación, el organismo de certificación debe confirmar el certificado o expedir uno nuevo con una fecha de expiración prorrogada. Si la revaluación no es satisfactoria, el organismo de certificación debe retirar el certificado y, en su caso, expedir uno nuevo con un ámbito de aplicación diferente. Dichas disposiciones deben aplicarse *mutatis mutandis* a la revaluación de los perfiles de protección.

(7) 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. Dichos documentos deben actualizarse para reflejar los últimos avances, como los relacionados con la evolución tecnológica, el panorama de las ciberamenazas, las prácticas sectoriales o las normas internacionales. Esta actualización resulta oportuna para los documentos del estado de la técnica relativos a los requisitos mínimos de seguridad de las instalaciones, la aplicación del potencial de ataque a tarjetas inteligentes, la aplicación del potencial de ataque a dispositivos de *hardware* con cajas de seguridad, la aplicación de los criterios comunes a los circuitos integrados y la evaluación de productos compuestos para tarjetas inteligentes y dispositivos similares. Asimismo, no se incluyen los documentos del estado de la técnica relativos a la evaluación y certificación de productos compuestos que utilizan la última versión de las normas de los criterios comunes, la reutilización de los resultados de la evaluación de las auditorías *in situ* y las aclaraciones sobre la interpretación de los perfiles de protección relativos a los dispositivos cualificados de creación de firma electrónica, los tacógrafos y los módulos de seguridad de *hardware*. A fin de garantizar una evaluación uniforme de los productos de TIC en el marco del EUCC, debe modificarse el anexo I para incluir dichos documentos nuevos y actualizados del estado de la técnica tras ser aprobados por el Grupo Europeo de Certificación de la Ciberseguridad (GECC).

(8) Además, debe añadirse al esquema el documento del estado de la técnica titulado «ADV_SPM.1 interpretation for CC:2022 transition» [«Interpretación ADV_SPM.1 para la transición CC:2022»] para garantizar que los procesos de certificación basados en perfiles de protección específicos puedan seguir utilizando la modelización formal (ADV_SPM.1) hasta que se actualicen los perfiles de protección correspondientes, por ejemplo, con la adición de una configuración de perfil de protección de garantías múltiples conforme con el CC:2022 que admita ADV_SPM.1. A fin de que el mercado disponga de tiempo suficiente para la transición hacia las normas actualizadas sobre criterios comunes, deben preverse normas de transición específicas para los perfiles de protección «Security IC Platform PP with Augmentation Packages (v1.0)» [«PP para plataformas de circuitos integrados de seguridad con paquetes de ampliación»], BSI-CC-PP-0084-2014, «Java Card System – Closed Configuration (v3.1)» [«Sistema Java Card: configuración cerrada»], BSI-CC-PP-0101-V2-2020, o Java Card System – Open Configuration (v3.1) [«Sistema Java Card: configuración abierta»], BSI-CC-PP-0099-V2-2020 Para evitar perturbaciones del mercado, conviene establecer que el documento del estado de la técnica sobre la interpretación ADV_SPM.1 para la transición CC:2022 se aplique a los procesos de certificación iniciados antes de la adopción del presente Reglamento. No obstante, la aplicación de este documento debe limitarse estrictamente a lo necesario, teniendo en cuenta el tiempo necesario para finalizar la actualización de los perfiles de protección correspondientes. Más concretamente, para los procesos de certificación que utilicen los perfiles de protección Security IC Platform PP with Augmentation Packages (v1.0), BSI-CC-PP-0084-2014, o Java Card System – Closed Configuration (v3.1), BSI-CC-PP-0101-V2-2020, el documento del estado de la técnica debe aplicarse a los procesos iniciados antes del 1 de octubre de 2026. En el caso de los procesos de certificación que utilicen el perfil de protección Java Card System – Open Configuration (v3.1), BSI-CC-PP-0099-V2-2020, el documento del estado de la técnica solo debe aplicarse a los procesos iniciados antes de la fecha de entrada en vigor del presente Reglamento, habida cuenta de que ya está disponible una nueva versión de dicho perfil de protección.

(9) Modificar los documentos del estado de la técnica durante un proceso de certificación podría perturbar la evaluación del producto y retrasar la expedición del certificado. Por lo tanto, se necesitan normas de transición adecuadas para los documentos nuevos o actualizados del estado de la técnica que permitan que los vendedores, las ITSEF, los organismos de certificación y otras partes interesadas realicen los ajustes necesarios. Los documentos actualizados y nuevos del estado de la técnica aplicables deben referirse a las solicitudes de certificación, incluidas las solicitudes de revaluación, mientras que, en los procesos de certificación en curso, debe seguir siendo posible utilizar versiones anteriores de los documentos del estado de la técnica.

(10) En los anexos II y III del Reglamento de Ejecución (UE) 2024/482 se enumeran, respectivamente, los perfiles de protección certificados en el nivel AVA_VAN 4 o 5 y los perfiles de protección recomendados. Debido a una actualización de los perfiles de protección, varias referencias están incompletas u obsoletas. Deben completarse dichas referencias, además de incluir otras nuevas para garantizar una cobertura más completa de los circuitos integrados seguros, las tarjetas inteligentes y los dispositivos conexos, así como de la computación segura.

(11) Es necesario introducir modificaciones en el artículo 19 del Reglamento de Ejecución (UE) 2024/482 para aclarar que el anexo IV se aplica, con los cambios necesarios, a la revisión de los certificados EUCC para los perfiles de protección.

(12) Dado que la declaración de seguridad es un elemento clave para comprender el alcance de un proceso de certificación, es también necesario que ENISA publique en su sitio web la declaración de seguridad correspondiente a cada certificado EUCC.

(13) Además, los organismos de certificación deben facilitar a ENISA una versión en inglés de la declaración de seguridad y del informe de certificación para que la Agencia pueda proporcionar dicha información en inglés en el sitio web correspondiente, de conformidad con el artículo 42, apartado 2, del Reglamento de Ejecución (UE) 2024/482. Por este motivo, los solicitantes de certificación deben facilitar a los organismos de certificación una versión en inglés de la declaración de seguridad, siempre que se les solicite.

(14) No es necesario que en la identificación única del certificado aparezca la referencia al nombre del organismo de certificación, ya que el número de identificación del organismo de certificación basta para identificar a dicho organismo de manera única. Tampoco es necesario que aparezca el mes de expedición, ya que el cómputo de los certificados se realiza anualmente. Así pues, dicho requisito debe suprimirse a efectos de simplificación. Dado que el año de expedición del certificado corresponde a la expedición del primer certificado, esa misma fecha debe figurar en la identificación única de los certificados expedidos tras una revisión, a fin de garantizar la trazabilidad.

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

(16) 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, se añaden los puntos 16, 17 y 18 siguientes:

«16) "serie de productos": conjunto de productos de TIC de un solicitante que utilizan la misma base funcional para satisfacer las mismas necesidades de seguridad, y cuyo diseño, *hardware*, *firmware* o programa informático pueden variar de un producto de TIC a otro;

17) "modificación menor": todo cambio en el objeto de evaluación certificado o en su entorno que no afecta negativamente a la garantía indicada en el certificado EUCC;

18) "modificación importante": todo cambio en el objeto de evaluación certificado o en su entorno que puede afectar negativamente a la garantía indicada en el certificado EUCC.».

2) En el artículo 5, se añade el apartado 3 siguiente:

«3. Un organismo de certificación podrá permitir la certificación de una serie de productos.».

3) En el artículo 9, apartado 2, la letra a) se sustituye por el texto siguiente:

«a) proporcionar al organismo de certificación y a la ITSEF toda la información necesaria, completa y correcta, y facilitar la información adicional necesaria que se le solicite, incluida una versión en inglés de la declaración de seguridad;».

4) En el artículo 11, apartado 3, la letra b) se sustituye por el texto siguiente:

«b) la identificación única del certificado, consistente en:

1) el nombre del esquema;

2) el número de identificación, de conformidad con el artículo 3 del Reglamento de Ejecución (UE) 2024/3143, del organismo de certificación que haya expedido el certificado;

3) el año de expedición del certificado inicial;

4) el número de identificación asignado por el organismo de certificación que haya expedido el certificado.».

5) En el artículo 19, el apartado 1 se sustituye por el texto siguiente:

«1. A petición del titular del certificado o por otros motivos justificados, el organismo de certificación podrá decidir revisar el certificado EUCC de un perfil de protección. La revisión se llevará a cabo de conformidad con el anexo IV. El organismo de certificación determinará el alcance de la revisión. Cuando sea necesario a efectos de la revisión, el organismo de certificación solicitará a la ITSEF que lleve a cabo una revaluación del perfil de protección certificado.».

6) El artículo 42 se modifica como sigue:

a) en el apartado 1, se añade la letra i) siguiente:

«i) la declaración de seguridad correspondiente a cada certificado EUCC;»;

b) el apartado 2 se sustituye por el texto siguiente:

«2. La información a que se refiere el apartado 1 deberá publicarse, como mínimo, en inglés. A tal fin, los organismos de certificación facilitarán a ENISA las versiones lingüísticas originales de los informes de certificación y de las declaraciones de seguridad; también proporcionarán la versión inglesa de dichos documentos sin demora injustificada.».

7) En el artículo 48, el apartado 4 se sustituye por el texto siguiente:

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

8) El anexo I se sustituye por el texto del anexo I del presente Reglamento.

9) El anexo II se sustituye por el texto del anexo II del presente Reglamento.

10) El anexo III se sustituye por el texto del anexo III del presente Reglamento.

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

12) El anexo V se modifica de conformidad con el anexo V del presente Reglamento.

13) El anexo IX se sustituye por el texto del anexo VI 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 8 de diciembre de 2025.

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 2;
      3) Reusing evaluation results of site audits (STAR) ["Reutilización de los resultados de las evaluaciones de las auditorías *in situ*"], versión 1;
      4) Application of Common Criteria to integrated circuits ["Aplicación de los criterios comunes a los circuitos integrados"], versión 2;
      5) 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;
      6) Certification of "open" smart card products ["Certificación de productos de tarjeta inteligente 'abierta'"], versión 1.1;
      7) Composite product evaluation for smart cards and similar devices for CC3.1 ["Evaluación de productos compuestos para tarjetas inteligentes y dispositivos similares para CC3.1"], versión 2;
      8) Composite product evaluation and certification for CC:2022 ["Evaluación y certificación de productos compuestos para CC:2022"], versión 1;
      9) Application of Attack Potential to Smartcards and Similar Devices ["Aplicación de potencial de ataque a tarjetas inteligentes y dispositivos similares"], versión 2;
      10) Security Evaluation and Certification of Qualified Electronic Signature/Seal Creation Devices ["Evaluación y certificación de dispositivos cualificados de creación de firma electrónica y sellos"], versión 1;
      11) ADV_SPM.1 interpretation for CC:2022 transition ["Interpretación ADV_SPM.1 para la transición CC:2022"], versión 1.1, aplicable a los procesos de certificación que usan los siguientes perfiles de protección:
         a) perfiles de protección Security IC Platform PP with Augmentation Packages ["Perfil de protección con paquetes de ampliación para plataformas de circuitos integrados de seguridad"] (v1.0) BSI-CC-PP-0084-2014, o Java Card System – Closed Configuration ["Sistema Java Card: configuración cerrada"] (v3.1) BSI-CC-PP-0101-V2-2020, iniciados con anterioridad al 1 de octubre de 2026;
         b) perfil de protección Java Card System – Open Configuration ["Sistema Java Card: configuración abierta"] (v3.1) BSI-CC-PP-0099-V2-2020, iniciado con anterioridad al 29 de diciembre de 2025.
   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 2;
      3) Reusing evaluation results of site audits (STAR) ["Reutilización de los resultados de las evaluaciones de las auditorías *in situ*"], versión 1;
      4) Application of Attack Potential to Hardware Devices with Security Boxes ["Aplicación de potencial de ataque a dispositivos de *hardware* con cajas de seguridad"], versión 2;
      5) Hardware assessment in UNE EN 419221-5 (HSM PP) ["Evaluación del *hardware* en UNE EN 419221-5 (HSM PP)"], versión 1;
      6) JIL Tachograph MS PP Clarification ["Aclaración del perfil de protección del sensor de movimiento del tacógrafo (JIL)"], versión 1.

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

«*ANEXO II*

Perfiles de protección certificados en los niveles AVA_VAN 4 o 5

1. Para dispositivos de creación de firmas y sellos cualificados a distancia:

   a) UNE-EN 419241-2: 2019 “Sistemas confiables que permiten firma de servidor. Parte 2: Perfil de protección de QSCD para la firma del servidor”, v0.16, ANSSI-CC-PP-2018/02-M01;

   b) UNE-EN 419221-5:2018 “Perfiles de protección para los módulos criptográficos de proveedores de servicios de confianza. Parte 5: Módulo criptográfico para servicios de confianza”, v0.15, ANSSI-CC-PP-2016/05-M01.

2. Perfiles de protección adoptados como documentos del estado de la técnica:

   [EN BLANCO].»

ANEXO III

«ANEXO III

Perfiles de protección recomendados

Perfiles de protección utilizados en la certificación de productos de TIC, incluidos los productos en los siguientes ámbitos técnicos:

1. Tarjetas inteligentes y dispositivos similares
   a) Pasaporte:
      1) PP Machine Readable Travel Document with "ICAO Application" Basic Access Control ["PP para documentos de viaje de lectura mecánica con control de acceso básico basado en la aplicación de las normas de la OACI"], v1.10, BSI-CC-PP-0055-2009;
      2) PP Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE_PP) ["Perfil de protección (PP) para documentos de viaje de lectura mecánica con procedimiento ordinario de inspección basado en PACE (establecimiento de conexión autenticada mediante contraseña)"], v1, BSI-CC-PP-0068-V2-2011-MA-01;
      3) PP Machine Readable Travel Document with "ICAO Application" Extended Access Control with PACE ["PP para documentos de viaje de lectura mecánica con control de acceso ampliado basado en la aplicación de las normas de la OACI con PACE"], v1.3, BSI-CC-PP-0056-V2-2012-MA-02;
   b) Dispositivos seguros de creación de firma:
      1) UNE-EN 419211-2:2013 "Perfiles de protección para los dispositivos seguros de creación de firma. Parte 2: Dispositivo con generación de claves", v1.03, BSI-CC-PP-0059-2009-MA-02;
      2) UNE-EN 419211-3:2013 "Perfiles de protección para los dispositivos seguros de creación de firma. Parte 3: Dispositivo con importación de claves", v1.0.2, BSI-CC-PP-0075-2012-MA-01;
      3) UNE-EN 419211-4:2013 "Perfiles de protección para los dispositivos seguros de creación de firma. Parte 4: Extensión para el dispositivo con generación de claves y comunicación confiada con la aplicación de generación de certificado", v1.0.1, BSI-CC-PP-0071-2012-MA-01;
      4) UNE-EN 419211-5:2013 "Perfiles de protección para los dispositivos seguros de creación de firma. Parte 5: Extensión para el dispositivo con generación de claves y comunicación confiada con la aplicación de creación de firma", v1.0.1, BSI-CC-PP-0072-2012-MA-01;
      5) UNE-EN 419211-6:2014 "Perfiles de protección para los dispositivos seguros de creación de firma. Parte 6: Extensión para el dispositivo con importación de claves y comunicación confiada con la aplicación de creación de firma", v1.0.4, BSI-CC-PP-0076-2013-MA-01;
   c) Tacógrafo: Digital Tachograph – Tachograph Card (TC PP) ["Tacógrafo digital: tarjeta de tacógrafo"], v1.0, BSI-CC-PP-0091-2017;
   d) Circuitos integrados seguros, plataforma Java Card y tarjeta universal de circuito integrado incorporada (eUICC):
      1) Universal SIM Java Card Platform Protection Profile Basic and SCWS Configurations ["Configuraciones básica y de servidor web de tarjeta inteligente del perfil de protección de la plataforma Java Card SIM universal"], v2.0.2, ANSSI-CC-PP-2010/04 (básica), ANSSI-CC-PP-2010/05 (básica y de servidor web de tarjeta inteligente);
      2) Security IC Platform PP with Augmentation Packages, ["Perfil de protección con paquetes de ampliación para plataformas de circuitos integrados de seguridad"], v1.0, BSI-CC-PP-0084-2014;
      3) Embedded UICC (eUICC) for Machine-to-Machine Devices ["Tarjeta universal de circuito integrado incorporada (eUICC) para dispositivos de máquina a máquina"], v1.1, BSI-CC-PP-0089-2015;
      4) Cryptographic Service Provider – CSP ["Proveedor de servicios criptográficos: CSP"], v0.9.8, BSI-CC-PP-0104-2019;
      5) Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au) ["Proveedor de servicios criptográficos: servicios de sello de tiempo y auditoría (PPC-CSP-TS-Au)"], v0.9.5, BSI-CC-PP-0107-2019;
      6) Configuration Cryptographic Service Provider – Time Stamp Service, Audit and Clustering (PPC-CSP-TS-Au-Cl) ["Proveedor de servicios criptográficos: servicios de sello de tiempo, auditoría y agrupamiento (PPC-CSP-TS-Au-Cl)"], v0.9.4, BSI-CC-PP-0108-2019;
      7) Java Card System – Closed Configuration ["Sistema Java Card: configuración cerrada"], v3.1, BSI-CC-PP-0101-V2-2020;
      8) Secure Element Protection Profile – GPC_SPE_174 ["Perfil de protección de elemento seguro"], v1.0, CCN-CC-PP-5-2021;
      9) Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile ["Perfil de protección de subsistema seguro en sistema en un chip (3S en SoC)"], v1.8, BSI-CC-PP-0117-V2-2023;
      10) Java Card System – Open Configuration ["Sistema Java Card: configuración abierta"], v3.2 BSI-CC-PP-0099-V3-2024;
      11) Embedded UICC for Consumer Devices Protection Profile ["Perfil de protección de tarjeta universal de circuito integrado incorporada para dispositivos de consumo"], v2.1, BSI-CC-PP-0100-V2-2025;
   e) Módulo de plataforma segura: Protection Profile PC Client Specific Trusted Platform Module Specification Family 2.0; Level 0; Revision 1.59 ["Perfil de protección para módulo de plataforma segura específico para cliente de PC, familia de especificación 2.0, nivel 0, revisión 1.59"], v1.3, ANSSI-CC-PP-2021/02.

2. Dispositivos de *hardware* con cajas de seguridad

   a) puntos de interacción (de pago) y terminales de pago [disponibles en inglés]:

      1) Punto de interacción “POI-CHIP-ONLY”, v4.0, ANSSI-CC-PP-2015/01;

      2) Punto de interacción “POI-CHIP-ONLY and Open Protocol Package” [“POI-CHIP-ONLY y paquete de protocolos abiertos”], v4.0, ANSSI-CC-PP-2015/02;

      3) Punto de interacción “POI-COMPREHENSIVE”, v4.0, ANSSI-CC-PP-2015/03;

      4) Punto de interacción “POI-COMPREHENSIVE and Open Protocol Package” [“POI-COMPREHENSIVE y paquete de protocolos abiertos”], v4.0, ANSSI-CC-PP-2015/04;

      5) Punto de interacción “POI-PED-ONLY”, v4.0, ANSSI-CC-PP-2015/05;

      6) Punto de interacción “POI-PED-ONLY and Open Protocol Package” [“POI-PED-ONLY y paquete de protocolos abiertos”], v4.0, ANSSI-CC-PP-2015/06;

   b) Módulo de seguridad de *hardware*:

      1) Cryptographic Module for CSP Signing Operations with Backup [“Módulo criptográfico para operaciones de firma de proveedores de servicios de certificación (PSC) con copia de seguridad (‘PP CMCSOB’)”], PP CMCSOB 14167-2, v0.35, ANSSI-CC-PP-2015/08;

      2) Cryptographic Module for CSP Key Generation Services [“Módulo criptográfico para servicios de generación de claves de proveedores de servicios de certificación (PSC) (‘PP CMCKG’)”], PP CMCKG 14167-3, v0.20, ANSSI-CC-PP-2015/09;

      3) Cryptographic Module for CSP Signing Operations without Backup [“Módulo criptográfico para operaciones de firma de proveedores de servicios de certificación (PSC) sin copia de seguridad (‘PP CMCSO’)”], PP CMCSO 14167-4, v0.32, ANSSI-CC-PP-2015/10;

   c) Tacógrafo:

      1) Digital Tachograph – Motion Sensor (PP MS) [“Tacógrafo digital: sensor de movimiento (PP MS)”], v1.0, BSI-CC-PP-0093-2017;

      2) Digital Tachograph – Vehicle Unit (PP VU) [“Tacógrafo digital: unidad intravehicular (PP VU)”], v1.15, BSI-CC-PP-0094-V2-2021;

      3) Digital Tachograph – External GNSS Facility (PP EGF) [“Tacógrafo digital: dispositivo GNSS externo (PP EGF)”], v1.10, BSI-CC-PP-0092-V2-2021;

3. Otros: Trusted Execution Environment Protection Profile [“Perfil de protección de entorno de ejecución fiable”], GPD_SPE_021, v1.3, ANSSI-CC-PP-2014/01-M02.’

ANEXO IV

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

1. En la sección IV.2, el punto 4 se sustituye por el texto siguiente:

«4. El organismo de certificación revisará el informe técnico de evaluación actualizado y elaborará un informe de revaluación. A continuación, se modificará el estado del certificado inicial con arreglo a lo dispuesto en el artículo 13 o en el artículo 19. Si la revaluación es satisfactoria, se aplica el artículo 13, apartado 2, letras a) o c), en el caso de la certificación de un producto, o el artículo 19, apartado 2, letras a) o c), en el caso de la certificación de un perfil de protección. Si la revaluación no es satisfactoria, se aplica el artículo 13, apartado 2, letras b) o d), en el caso de la certificación de un producto, o el artículo 19, apartado 2, letras b) o d), en el caso de la certificación de un perfil de protección.».

2. La sección IV.3 se modifica como sigue:

a) el título de la sección IV.3 se sustituye por el texto siguiente:

«IV.3 **Modificaciones de un producto de TIC certificado: mantenimiento y revaluación**»;

b) los puntos 4 y 5 se sustituyen por el texto siguiente:

«4. Tras dicho examen, el organismo de certificación calificará la magnitud de cada modificación como menor o importante en función de sus efectos en la garantía indicada en el certificado EUCC.

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, de conformidad con el artículo 13, apartado 2, letra a), o el artículo 19, apartado 2, letra a), y se elaborará un informe de mantenimiento del informe de certificación inicial.»;

c) se inserta el punto 5 *bis* siguiente:

«5 *bis*. En caso de que se efectúen modificaciones de las medidas de garantía en el entorno de desarrollo, incluida la adición de los requisitos de garantía de la familia CC ALC_FLR (corrección de defectos), el organismo de certificación puede solicitar a la ITSEF que lleve a cabo la evaluación de un subconjunto de las medidas de garantía afectadas. La ITSEF publicará un informe técnico de evaluación parcial, en el que se basará el organismo de certificación para confirmar si las modificaciones son importantes o menores. Cuando el organismo de certificación haya confirmado que las modificaciones son menores, será de aplicación el anexo IV, sección IV.3, punto 5. Cuando el organismo de certificación haya confirmado que las modificaciones son importantes, será de aplicación el anexo IV, sección IV.3, punto 7.».

ANEXO V

El punto V.1 del anexo V del Reglamento de Ejecución (UE) 2024/482 se sustituye por el texto siguiente:

«V.1 **Informe de certificación**

1. A partir de los informes técnicos de evaluación facilitados por la ITSEF, el organismo de certificación elaborará un informe de certificación que se publicará junto con el certificado EUCC correspondiente y la declaración de seguridad.

2. El informe de certificación es la fuente de información detallada y práctica sobre el producto de TIC y sobre el despliegue seguro de dicho producto o productos, por lo que incluirá toda la información públicamente accesible y compartible que resulte pertinente para los usuarios y las partes interesadas. También puede contener referencias a dicha información públicamente accesible y compartible.

3. El informe de certificación contendrá como mínimo la siguiente información:

   a) resumen;

   b) identificación del producto de TIC;

   c) información de contacto relacionada con la evaluación del producto de TIC;

   d) políticas de seguridad;

   e) hipótesis y aclaración del ámbito de aplicación;

   f) información arquitectónica;

   g) información complementaria sobre ciberseguridad, en su caso;

   h) resumen de la evaluación del producto de TIC y configuración evaluada;

   i) resultados de la evaluación e información relativa al certificado;

   j) comentarios y recomendaciones, en su caso;

   k) anexos, en su caso;

   l) referencia a la declaración de seguridad del producto de TIC presentado para su certificación;

   m) en su caso, la marca o etiqueta asociada al esquema;

   n) glosario, en su caso;

   o) bibliografía.

4. El resumen a que se refiere el apartado 3, letra a), será una breve recapitulación de todo el informe de certificación. Ofrecerá una visión general clara y concisa de los resultados de la evaluación y contendrá la siguiente información:

   a) denominación del producto de TIC evaluado;

   b) nombre de la ITSEF que haya llevado a cabo la evaluación;

   c) fecha de conclusión de la evaluación;

   d) fecha de expedición del certificado;

   e) en su caso, año de expedición del certificado inicial;

   f) período de validez;

   g) identificación única del certificado, tal como se describe en el artículo 11;

   h) breve descripción de los resultados del informe de certificación, que incluya:

      i) la versión y, en su caso, edición de los criterios comunes aplicada a la evaluación;

      ii) la lista de los componentes de garantía de seguridad o el paquete de garantía de los criterios comunes, el nivel AVA_VAN aplicado durante la evaluación y el respectivo nivel de garantía, con arreglo a lo dispuesto en el artículo 52 del Reglamento (UE) 2019/881, al que se refiere el certificado EUCC;

      iii) cuando proceda, el perfil o los perfiles de protección con los que el producto de TIC declara su conformidad;

      iv) la referencia a la política de seguridad del producto de TIC evaluado;

      v) la cláusula o las cláusulas de exención de responsabilidad, en su caso.

5. La identificación a que se refiere el apartado 3, letra b), deberá identificar claramente el producto de TIC evaluado e incluir la siguiente información:

   a) identificación única del producto de TIC evaluado;

   b) enumeración de los componentes del producto de TIC que forman parte de la evaluación, con el número de versión de cada componente;

   c) referencia a requisitos adicionales para el entorno operativo del producto de TIC certificado.

6. La información de contacto a que se refiere el apartado 3, letra c), contendrá, como mínimo, los elementos siguientes:

   a) nombre del desarrollador;

   b) nombre e información de contacto del titular del certificado EUCC;

   c) nombre del organismo de certificación que haya expedido el certificado;

   d) autoridad nacional de certificación de la ciberseguridad responsable;

   e) nombre de la ITSEF que ha llevado a cabo la evaluación y, en su caso, lista de subcontratistas.

7. La política de seguridad a que se refiere el apartado 3, letra d), contendrá la descripción de la política de seguridad del producto de TIC como conjunto de servicios de seguridad, así como de las políticas o normas que el producto de TIC evaluado deba aplicar o cumplir. También incluirá la siguiente información:

   a) una descripción de los procesos de gestión de vulnerabilidades y divulgación de vulnerabilidades del titular del certificado, que debe completarse únicamente con información que pueda divulgarse;

   b) la política de continuidad de la garantía del titular del certificado, en donde se incluya, cuando proceda, la descripción de los procesos de producción o de gestión del ciclo de vida del titular del certificado, de conformidad con el anexo IV, sección IV.1;

   c) en su caso, la presencia de un procedimiento de gestión de parches y el resultado de su evaluación de conformidad con el anexo IV, sección IV.4;

8. Las hipótesis y la aclaración del ámbito de aplicación a que se refiere el apartado 3, letra e), contendrá información sobre las circunstancias y los objetivos relacionados con el uso previsto del producto a que se refiere el artículo 7, apartado 1, letra c), en particular:

   a) hipótesis sobre el uso y el despliegue del producto de TIC en forma de requisitos mínimos, como el cumplimiento de requisitos adecuados de instalación, configuración y *hardware*;

   b) hipótesis sobre el entorno para el correcto funcionamiento del producto de TIC;

   c) descripción de cualquier amenaza para el producto de TIC que no esté contrarrestada por las funciones de seguridad evaluadas del producto en función de su uso previsto, si se considera pertinente para un usuario potencial de un producto de TIC.

   La información a que se refiere el párrafo primero será lo más clara y comprensible posible para que los usuarios potenciales del producto de TIC certificado puedan tomar decisiones con conocimiento de causa sobre los riesgos asociados a su uso.

9. La información arquitectónica a que se refiere el apartado 3, letra f), contendrá una descripción de alto nivel del producto de TIC y de sus principales componentes, sobre la base de los entregables definidos en la familia de garantía de los criterios comunes: Development — TOE Design [«Desarrollo — Diseño del objeto de evaluación»] (ADV_TDS).

10. La información adicional sobre la ciberseguridad a que se refiere el apartado 3, letra g), contendrá el enlace al sitio web del titular del certificado EUCC, tal como se contempla en el artículo 55 del Reglamento (UE) 2019/881.

11. En la evaluación y la configuración del producto de TIC a que se refiere el apartado 3, letra h), se describirán las actividades de ensayo tanto del desarrollador como del evaluador, indicando el enfoque, la configuración y la escala del ensayo. Figurará, como mínimo. la información siguiente:

    a) especificación de los componentes de garantía utilizados con arreglo a las normas a que se refiere el artículo 3;

    b) versión de los documentos del estado de la técnica y demás criterios de evaluación de la seguridad utilizados en la evaluación;

    c) ajustes y configuración del objeto de evaluación empleados en los ensayos y los análisis de vulnerabilidades;

    d) todo perfil de protección que se haya utilizado, especificando la siguiente información: denominación, versión, fecha y certificado del perfil de protección.

12. Los resultados de la evaluación y la información relativa al certificado a que se refiere el apartado 3, letra i), contendrán información sobre el nivel de garantía alcanzado, tal como se indica en el artículo 4 del presente Reglamento y el artículo 52 del Reglamento (UE) 2019/881.

13. Los comentarios y las recomendaciones contemplados en el apartado 3, letra j), se utilizarán para proporcionar información adicional sobre los resultados de la evaluación. Dichos comentarios y recomendaciones podrán referirse a deficiencias del producto de TIC descubiertas durante la evaluación o consistir en indicaciones de características particularmente útiles.

14. Los anexos a que se refiere el apartado 3, letra k), se emplearán para precisar toda la información adicional que pueda resultar de utilidad a los destinatarios del informe, pero que no pueda incluirse de forma lógica en sus secciones obligatorias, también en el caso de una descripción completa de una política de seguridad.

15. La declaración de seguridad a que se refiere el apartado 3, letra l), hará referencia a la declaración de seguridad evaluada. La declaración de seguridad evaluada se facilitará junto con el informe de certificación a efectos de publicación en el sitio web contemplado en el artículo 50, apartado 1, del Reglamento (UE) 2019/881. Si es necesario editar la declaración de seguridad evaluada antes de que se publique, se hará de conformidad con el anexo V, punto V.2, del presente Reglamento.

16. Las marcas o etiquetas asociadas al esquema EUCC a que se refiere el apartado 3, letra m), se insertarán en el informe de certificación de conformidad con las normas y los procedimientos establecidos en el artículo 11.

17. El glosario contemplado en el apartado 3, letra n), se utilizará para facilitar la lectura del informe, al proporcionar definiciones de acrónimos o términos cuyo significado pueden no resultar obvios.

18. La sección de bibliografía a que se refiere el apartado 3, letra o), incluirá referencias a todos los documentos utilizados en la elaboración del informe de certificación. Dicha información incluirá, como mínimo, lo siguiente:

    a) los criterios de evaluación de la seguridad, los documentos del estado de la técnica y otras especificaciones pertinentes utilizadas;

    b) el informe técnico de evaluación;

    c) el informe técnico de evaluación para la evaluación de un producto compuesto, en su caso;

    d) la documentación de referencia técnica;

    e) las orientaciones en materia de seguridad del desarrollador;

    f) la lista de configuración de los desarrolladores.

    Con el fin de garantizar la reproducibilidad de la evaluación, toda la documentación citada debe identificarse de manera inequívoca con su respectiva fecha de publicación y su respectivo número de versión.».

ANEXO VI

«ANEXO IX

Marca y etiqueta

1. Formato de la marca y la etiqueta:

2. Si se reducen o amplían la marca y la etiqueta, deberán respetarse las proporciones facilitadas en el punto 1.

3. En caso de colocarse físicamente, la marca y la etiqueta tendrán una altura mínima de 5 mm.».