2024/482

7.2.2024

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)

(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 presente Reglamento 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. El EUCC se fundamenta en el Acuerdo de reconocimiento mutuo (en lo sucesivo, «ARM») de los certificados de seguridad de las tecnologías de la información adoptado por el Grupo de Altos Funcionarios sobre Seguridad de los Sistemas de Información (en lo sucesivo, «SOG-IS») ([2]) con arreglo a los criterios comunes, incluidos los procedimientos y documentos del grupo.

(2) El esquema debe basarse en las normas internacionales establecidas. Los criterios comunes son una norma internacional para la evaluación de la seguridad de la información, publicada, por ejemplo, como ISO/IEC 15408 «Seguridad de la información, ciberseguridad y protección de la privacidad. Criterios de evaluación para la seguridad de las tecnologías de la información», que se basa en la evaluación por un tercero y contempla siete niveles de aseguramiento de la evaluación. Los criterios comunes van acompañados de la metodología común de evaluación, publicada, por ejemplo, como ISO/IEC 18045 «Seguridad de la información, ciberseguridad y protección de la privacidad. Criterios de evaluación para la seguridad de las tecnologías de la información. Metodología para la evaluación de la seguridad de las tecnologías de la información». Las especificaciones y los documentos que apliquen las disposiciones del presente Reglamento podrán referirse a una norma de acceso público que se asemeje a la utilizada para certificar en virtud del presente Reglamento, como los criterios comunes para la evaluación de la seguridad de las tecnologías de la información y la metodología común para la evaluación de la seguridad de las tecnologías de la información.

(3) El EUCC utiliza los componentes del 1 al 5 de la familia de evaluación de vulnerabilidad de los criterios comunes (AVA_VAN). Estos cinco componentes proporcionan todos los principales determinantes y dependencias para analizar las vulnerabilidades de los productos de tecnologías de la información y la comunicación (en lo sucesivo, «TIC»). Dado que los componentes se corresponden con los niveles de garantía contemplados en el presente Reglamento, permiten elegir con conocimiento de causa el nivel de garantía, sobre la base de las evaluaciones llevadas a cabo de los requisitos de seguridad y del riesgo asociado al uso previsto del producto de TIC. El solicitante de un certificado EUCC debe presentar la documentación relacionada con el uso previsto del producto de TIC y el análisis de los niveles de riesgo asociados a dicho uso, con el fin de que el organismo de evaluación de la conformidad pueda evaluar la idoneidad del nivel de garantía seleccionado. Cuando las actividades de evaluación y de certificación las lleve a cabo el mismo organismo de evaluación de la conformidad, el solicitante debe presentar la información solicitada solo una vez.

(4) Un ámbito técnico es un marco de referencia que abarca un grupo de productos de TIC que poseen una funcionalidad de seguridad específica y similar que reduce los ataques cuando las características son comunes a un determinado nivel de garantía. Los ámbitos técnicos describen en documentos del estado de la técnica los requisitos específicos de seguridad, así como los métodos, las técnicas y los instrumentos de evaluación adicionales aplicables a la certificación de los productos de TIC comprendidos en cada ámbito técnico. Por lo tanto, también fomentan la

([1]) DO L 151 de 7.6.2019, p. 15.

([2]) Acuerdo de reconocimiento mutuo de los certificados de evaluación de la seguridad de las tecnologías de la información, versión 3.0 de enero de 2010, disponible en sogis.eu, aprobado por el Grupo de Altos Funcionarios sobre Seguridad de los Sistemas de Información de la Comisión Europea en respuesta al punto 3 de la Recomendación 95/144/CE del Consejo, de 7 de abril de 1995, relativa a los criterios comunes de evaluación de la seguridad en las tecnologías de la información (DO L 93 de 26.4.1995, p. 27).

armonización de la evaluación de los productos de TIC en cuestión. En la actualidad se utilizan ampliamente dos ámbitos técnicos para la certificación en los niveles AVA_VAN.4 y AVA_VAN.5. El primer ámbito técnico es el de «tarjetas inteligentes y dispositivos similares», en el que partes significativas de la funcionalidad de seguridad requerida dependen de elementos de *hardware* específicos, adaptados y a menudo separables (por ejemplo, *hardware* de tarjetas inteligentes, circuitos integrados, productos compuestos de tarjetas inteligentes, módulos de plataforma segura utilizados en computación segura o tarjetas de tacógrafos digitales). El segundo ámbito técnico es el de «dispositivos de *hardware* con cajas de seguridad», en el que partes significativas de la funcionalidad de seguridad requerida dependen de una carcasa o envolvente física del *hardware* (denominada «caja de seguridad») diseñada para resistir ataques directos, por ejemplo, terminales de pago, unidades intravehiculares de tacógrafos, contadores inteligentes, terminales de control de acceso y módulos de seguridad de *hardware*.

(5) Al solicitar la certificación, el solicitante debe relacionar su motivación para seleccionar un determinado nivel de garantía con los objetivos establecidos en el artículo 51 del Reglamento (UE) 2019/881 y con la selección de componentes del catálogo de requisitos funcionales de seguridad y requisitos de garantía de seguridad incluidos en los criterios comunes. Los organismos de certificación deben evaluar la adecuación del nivel de garantía elegido y garantizar que este refleje el nivel de riesgo asociado al uso previsto del producto de TIC.

(6) Con arreglo a los criterios comunes, la certificación se lleva a cabo de acuerdo con una declaración de seguridad que engloba una definición del problema de seguridad del producto de TIC, así como los objetivos de seguridad que abordan dicho problema. El problema de seguridad proporciona información sobre el uso previsto del producto de TIC y los riesgos asociados a este uso. Un conjunto selecto de requisitos de seguridad responde tanto al problema de seguridad como a los objetivos de seguridad de un producto de TIC.

(7) Así pues, los perfiles de protección constituyen un medio eficaz para predeterminar los criterios comunes aplicables a una determinada categoría de productos de TIC y, por tanto, también un elemento fundamental en el proceso de certificación de los productos de TIC comprendidos en cada uno de estos perfiles. Los perfiles de protección sirven para valorar las futuras declaraciones de seguridad correspondientes a la categoría específica de productos de TIC a la que se refiera cada perfil de protección. Además, racionalizan y mejoran la eficiencia del proceso de certificación de productos de TIC y ayudan a los usuarios a especificar de forma correcta y efectiva la funcionalidad de un producto de TIC. Por consiguiente, los perfiles de protección deben considerarse parte integrante del proceso de TIC que conduce a la certificación de productos de TIC.

(8) Con el fin de permitir que desempeñen su función en el proceso de TIC que apoye la elaboración y el suministro de un producto de TIC certificado, los propios perfiles de protección deben poder certificarse con independencia de la certificación del producto de TIC específico comprendido en el perfil de protección correspondiente. Así pues, al objeto de garantizar un alto nivel de ciberseguridad, resulta fundamental aplicar, como mínimo, el mismo nivel de control a los perfiles de protección que a las declaraciones de seguridad. Los perfiles de protección deben evaluarse y certificarse por separado del respectivo producto de TIC y únicamente mediante la aplicación de la clase de garantía de los criterios comunes y de la metodología común de evaluación correspondiente a los perfiles de protección («APE») y, en su caso, la correspondiente a las configuraciones de perfiles de protección («ACE»). Debido a su importante y delicada función de referencia en la certificación de los productos de TIC, solo deben ser certificados por organismos públicos o por un organismo de certificación que haya recibido la aprobación previa del perfil de protección específico por parte de la autoridad nacional de certificación de la ciberseguridad. Dado el papel fundamental que desempeñan en la certificación con nivel de garantía «elevado», en particular fuera de los ámbitos técnicos, los perfiles de protección deben confeccionarse como documentos del estado de la técnica que deben ser aprobados por el Grupo Europeo de Certificación de la Ciberseguridad.

(9) Los perfiles de protección certificados deben incluirse en el control de la conformidad y el cumplimiento por parte de las autoridades nacionales de certificación de la ciberseguridad. Cuando se disponga de la metodología, los instrumentos y las capacidades aplicadas a los métodos de evaluación de los productos de TIC para perfiles de protección certificados específicos, los ámbitos técnicos podrán basarse en dichos perfiles de protección específicos.

(10) Con miras a lograr un alto nivel de confianza y garantía en los productos de TIC certificados, no se debe permitir la autoevaluación en virtud del presente Reglamento, sino únicamente la evaluación de la conformidad por terceros por parte de instalaciones de evaluación de la seguridad de las tecnologías de la información y de organismos de certificación.

(11) La comunidad SOG-IS facilitó interpretaciones y enfoques conjuntos de aplicación de los criterios comunes y la metodología común de evaluación en la certificación, en particular para el nivel de garantía «elevado» que persiguen los ámbitos técnicos «tarjetas inteligentes y dispositivos similares» y «dispositivos de *hardware* con cajas de seguridad». La reutilización de estos documentos de apoyo en el esquema EUCC garantiza una transición fluida de los esquemas aplicados a escala nacional en el marco del ARM del SOG-IS al esquema armonizado EUCC. Así pues, deben incluirse en el presente Reglamento metodologías de evaluación armonizadas de importancia general para todas las actividades de certificación. Además, la Comisión debe poder solicitar al Grupo Europeo de Certificación de la Ciberseguridad que adopte un dictamen por el que se apruebe y recomiende la aplicación de las metodologías de evaluación especificadas en los documentos del estado de la técnica para la certificación del producto de TIC o del perfil de protección en virtud del esquema EUCC. Por consiguiente, en el anexo I del presente Reglamento se enumeran los documentos del estado de la técnica relativos a las actividades de evaluación llevadas a cabo por los organismos de evaluación de la conformidad. Corresponde al Grupo Europeo de Certificación de la Ciberseguridad aprobar y mantener dichos documentos. Los documentos del estado de la técnica deben utilizarse en la certificación. Solo en casos excepcionales y debidamente justificados, un organismo de evaluación de la conformidad podrá no utilizarlos, siempre que se cumplan determinadas condiciones, en particular la aprobación por parte de la autoridad nacional de certificación de la ciberseguridad.

(12) La certificación de los productos de TIC en los niveles AVA_VAN.4 o AVA_VAN.5 solo debe ser posible en determinadas condiciones y cuando se disponga de una metodología de evaluación específica. Esta podrá establecerse en documentos del estado de la técnica pertinentes en el ámbito técnico o en determinados perfiles de protección adoptados como documentos del estado de la técnica que sean pertinentes para la categoría de productos de que se trate. Solo en casos excepcionales y debidamente justificados, será posible la certificación en estos niveles de garantía, siempre que se cumplan determinadas condiciones, en particular la aprobación por parte de la autoridad nacional de certificación de la ciberseguridad, entre otros aspectos de la metodología de evaluación aplicable. Estos casos excepcionales y debidamente justificados pueden presentarse cuando la legislación nacional o de la Unión exija la certificación de un producto de TIC en los niveles AVA_VAN.4 o AVA_VAN.5. Del mismo modo, en casos excepcionales y debidamente justificados, los perfiles de protección podrán certificarse sin aplicar los documentos del estado de la técnica pertinentes, siempre que se cumplan determinadas condiciones, en particular la aprobación por parte de la autoridad nacional de certificación de la ciberseguridad, entre otros aspectos de la metodología de evaluación aplicable.

(13) Las marcas y etiquetas utilizadas en el marco del EUCC tienen por objeto demostrar de forma visible la fiabilidad del producto de TIC certificado a los usuarios y permitirles elegir con conocimiento de causa a la hora de adquirir productos de TIC. El uso de marcas y etiquetas también debe estar sujeto a las normas y condiciones establecidas en la norma ISO/IEC 17065 y, en su caso, en la norma ISO/IEC 17030 con las orientaciones aplicables.

(14) Los organismos de certificación deben decidir la duración de la validez de los certificados teniendo en cuenta el ciclo de vida del producto de TIC de que se trate. Dicha duración no debe ser superior a cinco años. Las autoridades nacionales de certificación de la ciberseguridad deben esforzarse por armonizar la duración de la validez en la Unión.

(15) Cuando se reduzca el ámbito de aplicación de un certificado EUCC existente, se retirará el certificado y se expedirá uno nuevo con el ámbito de aplicación correspondiente para garantizar que los usuarios estén claramente informados del ámbito de aplicación y del nivel de garantía actuales del certificado de un determinado producto de TIC.

(16) La certificación de perfiles de protección difiere de la certificación de productos de TIC, ya que atañe a un proceso de TIC. Habida cuenta de que cada perfil de protección abarca una determinada categoría de productos de TIC, su evaluación y certificación no pueden llevarse a cabo sobre la base de un único producto de TIC. Además, dado que un perfil de protección unifica los requisitos generales de seguridad correspondientes a una categoría de productos de TIC, con independencia de la manifestación del producto de TIC por parte de su vendedor, el período de validez de un certificado EUCC relativo a un perfil de protección debe, en principio, abarcar un mínimo de cinco años y puede prolongarse durante la duración del respectivo perfil de protección.

(17) Por «organismo de evaluación de la conformidad» se entiende un organismo que desempeña actividades de evaluación de la conformidad que incluyen calibración, ensayo, certificación e inspección. A fin de garantizar una alta calidad de los servicios, el presente Reglamento especifica que las actividades de ensayo, por una parte, y las actividades de certificación e inspección, por otra, deben llevarlas a cabo entidades que operen de forma independiente entre sí, a saber, instalaciones de evaluación de la seguridad de las tecnologías de la información («ITSEF») y organismos de certificación, respectivamente. Ambos tipos de organismos de evaluación de la conformidad deben estar acreditados y, en determinadas situaciones, obtener una autorización.

(18) Los organismos de certificación deben ser acreditados de conformidad con la norma ISO/IEC 17065 por el organismo nacional de acreditación para los niveles de garantía «sustancial» y «elevado». Además de la acreditación con arreglo al Reglamento (UE) 2019/881, en relación con el Reglamento (CE) n.º 765/2008, los organismos de evaluación de la conformidad deben cumplir requisitos específicos con el fin de garantizar su competencia técnica para la evaluación de los requisitos de ciberseguridad con nivel de garantía «elevado» en el marco del EUCC, lo que queda confirmado por una «autorización». A fin de prestar apoyo al proceso de autorización, ENISA debe elaborar y publicar los documentos del estado de la técnica pertinentes, previa aprobación del Grupo Europeo de Certificación de la Ciberseguridad.

(19) La competencia técnica de una ITSEF debe evaluarse mediante la acreditación del laboratorio de ensayo de conformidad con la norma ISO/IEC 17025, complementada por la norma ISO/IEC 23532-1 por lo que respecta a todo el conjunto de actividades de evaluación que resulten pertinentes para el nivel de garantía y se especifiquen en la norma ISO/IEC 18045 en relación con la norma ISO/IEC 15408. Tanto el organismo de certificación como la ITSEF deben establecer y mantener un sistema adecuado de gestión de competencias del personal inspirado en la norma ISO/IEC 19896-1 por lo que respecta a los elementos y niveles de competencia y a la evaluación de esta. En cuanto a los requisitos en materia de conocimientos, capacidades, experiencia y educación aplicables a los evaluadores, deben extraerse de la norma ISO/IEC 19896-3. Han de demostrarse las disposiciones y medidas equivalentes que aborden las desviaciones de dichos sistemas de gestión de competencias, con arreglo a los objetivos del sistema.

(20) Para obtener la autorización correspondiente, la ITSEF debe demostrar su capacidad de determinar la ausencia de las vulnerabilidades conocidas, la aplicación correcta y coherente de las funcionalidades de seguridad más avanzadas de la tecnología específica de que se trate y la resistencia del producto de TIC en cuestión a atacantes expertos. Además, por lo que respecta a las autorizaciones en el ámbito técnico de «tarjetas inteligentes y dispositivos similares», la ITSEF también debe demostrar las capacidades técnicas necesarias para las actividades de evaluación y las tareas conexas, tal como se definen en el documento de apoyo de los criterios comunes relativo a los requisitos mínimos aplicables a las ITSEF para las evaluaciones de seguridad de tarjetas inteligentes y dispositivos similares ([3]). Para la autorización en el ámbito técnico «dispositivos de *hardware* con cajas de seguridad», la ITSEF debe, asimismo, demostrar los requisitos técnicos mínimos necesarios para llevar a cabo las actividades de evaluación y las tareas conexas en dispositivos de *hardware* con cajas de seguridad, según lo recomendado por el Grupo Europeo de Certificación de la Ciberseguridad. En el contexto de los requisitos mínimos, la ITSEF debe ser capaz de llevar a cabo los diferentes tipos de ataques previstos en el documento de apoyo de los criterios comunes *Application of Attack Potential to Hardware Devices with Security Boxes* [«Aplicación de potencial de ataque a dispositivos de *hardware* con cajas de seguridad», en inglés]. Estas capacidades abarcan los conocimientos y las competencias del evaluador, así como el equipo y los métodos de evaluación necesarios para determinar y evaluar los diferentes tipos de ataques.

(21) La autoridad nacional de certificación de la ciberseguridad debe controlar el cumplimiento de los organismos de certificación, las ITSEF y los titulares de certificados con las obligaciones que les incumben en virtud del presente Reglamento y del Reglamento (UE) 2019/881, para lo cual debe servirse de toda fuente de información adecuada, incluida la información recabada de los participantes en el proceso de certificación y de las propias investigaciones.

(22) Los organismos de certificación deben cooperar con las autoridades de vigilancia del mercado pertinentes y tener en cuenta toda información sobre vulnerabilidades que pueda incumbir a los productos de TIC para los que hayan expedido certificados. Asimismo, deben supervisar los perfiles de protección que han certificado para determinar si los requisitos de seguridad establecidos para cada categoría de productos de TIC siguen reflejando la evolución más reciente del panorama de amenazas.

(23) En apoyo del control del cumplimiento, las autoridades nacionales de certificación de la ciberseguridad deben cooperar con las autoridades de vigilancia del mercado pertinentes de conformidad con el artículo 58 del Reglamento (UE) 2019/881 y el Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo ([4]). Los operadores económicos de la Unión están obligados a compartir información y cooperar con las autoridades de vigilancia del mercado, de conformidad con el artículo 4, apartado 3, del Reglamento (UE) 2019/1020.

([3]) Joint Interpretation Library: *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», documento en inglés], versión 2.1 de febrero de 2020, disponible en el sitio internet (sogis.eu).

([4]) Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativo a la vigilancia del mercado y la conformidad de los productos y por el que se modifican la Directiva 2004/42/CE y los Reglamentos (CE) n.º 765/2008 y (UE) n.º 305/2011 (DO L 169 de 25.6.2019, p. 1).

(24) Los organismos de certificación deben controlar el cumplimiento de los titulares de un certificado y la conformidad de todos los certificados expedidos en virtud del EUCC. Dicho control debe garantizar que todos los informes de evaluación facilitados por las ITSEF y las conclusiones adoptadas en ellos, así como los criterios y métodos de evaluación, se apliquen de manera coherente y correcta en todas las actividades de certificación.

(25) Cuando se detecten posibles problemas de incumplimiento que afecten a un producto de TIC certificado, es importante garantizar una respuesta proporcionada, por lo que se podrán suspender los certificados. Esta suspensión ha de conllevar una serie de restricciones sobre la promoción y el uso del producto de TIC en cuestión, pero no debe afectar a la validez del certificado. El titular del certificado de la UE debe notificar la suspensión a los compradores de los productos de TIC afectados, mientras que la autoridad nacional de certificación de la ciberseguridad competente se encargará de su comunicación a las autoridades de vigilancia del mercado pertinentes. Con objeto de informar al público, ENISA debe publicar la información relativa a una suspensión en un sitio web específico.

(26) El titular de un certificado EUCC debe aplicar los procedimientos necesarios de gestión de vulnerabilidades y garantizar que dichos procedimientos estén integrados en su organización. Cuando tenga conocimiento de una posible vulnerabilidad, el titular del certificado EUCC debe llevar a cabo un análisis del impacto de la vulnerabilidad. Si este análisis confirma que la vulnerabilidad puede aprovecharse, el titular del certificado debe enviar un informe de evaluación al organismo de certificación, que, a su vez, debe informar a la autoridad nacional de certificación de la ciberseguridad. Dicho informe debe explicar el impacto de la vulnerabilidad, las modificaciones o soluciones correctoras necesarias y también las posibles repercusiones más amplias de la vulnerabilidad, así como soluciones correctoras para otros productos. En caso necesario, la norma EN ISO/IEC 29147 debe complementar el procedimiento para la divulgación de vulnerabilidades.

(27) A efectos de la certificación, los organismos de evaluación de la conformidad y las autoridades nacionales de certificación de la ciberseguridad recaban datos confidenciales y delicados y secretos comerciales, también relacionados con la propiedad intelectual e industrial o el control del cumplimiento, que requieren una protección adecuada. Así pues, deben poseer las competencias y los conocimientos técnicos necesarios e instaurar sistemas para la protección de la información. Los requisitos y las condiciones para la protección de la información deben cumplirse tanto en los procedimientos de acreditación como en los de autorización.

(28) ENISA debe proporcionar la lista de perfiles de protección certificados en su sitio web de certificación de la ciberseguridad e indicar su situación, de conformidad con el Reglamento (UE) 2019/881.

(29) El presente Reglamento establece las condiciones aplicables a los acuerdos de reconocimiento mutuo con terceros países. Estos acuerdos pueden ser bilaterales o multilaterales y deben sustituir a acuerdos similares que estén en vigor. Con el fin de facilitar una transición fluida a dichos acuerdos de reconocimiento mutuo, los Estados miembros podrán mantener en vigor los acuerdos de cooperación con terceros países durante un período limitado.

(30) Los organismos de certificación que expidan certificados EUCC con un nivel de garantía «elevado», así como las ITSEF asociadas pertinentes, deben someterse a evaluaciones por pares. El objetivo de las evaluaciones por pares ha de ser determinar el cumplimiento permanente de la constitución y los procedimientos de un organismo de certificación evaluado por pares con los requisitos del esquema EUCC. Las evaluaciones por pares difieren de las revisiones entre pares entre las autoridades nacionales de certificación de la ciberseguridad, tal como se establece en el artículo 59 del Reglamento (UE) 2019/881. Las evaluaciones por pares deben confirmar que los organismos de certificación trabajan de forma armonizada y expiden certificados de la misma calidad, y deben detectar cualquier posible fortaleza o debilidad en el funcionamiento de los organismos de certificación, también con vistas a compartir las mejores prácticas. Habida cuenta de los diferentes tipos de organismos de certificación que existen, deben permitirse diferentes tipos de evaluación por pares. En casos más complejos, como el de los organismos de certificación que expiden certificados que abarquen niveles AVA_VAN diferentes, pueden utilizarse diferentes tipos de evaluación por pares, siempre que se cumplan todos los requisitos.

(31) El Grupo Europeo de Certificación de la Ciberseguridad debe desempeñar un papel importante en el mantenimiento del esquema, que ha de llevarse a cabo, entre otras cosas, mediante la cooperación con el sector privado, la creación de subgrupos especializados, y los trabajos preparatorios y la asistencia pertinentes que solicite la Comisión. El Grupo Europeo de Certificación de la Ciberseguridad desempeña un papel importante en la aprobación de documentos del estado de la técnica. Al aprobar y adoptar documentos del estado de la técnica, deben tenerse debidamente en cuenta los elementos mencionados en el artículo 54, apartado 1, letra c), del Reglamento

(UE) 2019/881. Los ámbitos técnicos y los documentos del estado de la técnica deben publicarse en el anexo I del presente Reglamento. Los perfiles de protección adoptados como documentos del estado de la técnica deben publicarse en el anexo II. A fin de garantizar que estos anexos sean dinámicos, la Comisión podrá modificarlos, de conformidad con el procedimiento establecido en el artículo 66, apartado 2, del Reglamento (UE) 2019/881, y teniendo en cuenta el dictamen del Grupo Europeo de Certificación de la Ciberseguridad. El anexo III contiene perfiles de protección recomendados que, en el momento de la entrada en vigor del presente Reglamento, no son documentos del estado de la técnica. Deben publicarse en el sitio web de ENISA al que se refiere el artículo 50, apartado 1, del Reglamento (UE) 2019/881.

(32) El presente Reglamento debe empezar a aplicarse doce meses después de su entrada en vigor. Los requisitos del capítulo IV y del anexo V no requieren un período transitorio y, por tanto, deben aplicarse a partir de la entrada en vigor del presente Reglamento.

(33) Las medidas previstas en el presente Reglamento se ajustan al dictamen del Comité Europeo de Certificación de la Ciberseguridad creado en virtud del artículo 66 del Reglamento (UE) 2019/881,

HA ADOPTADO EL PRESENTE REGLAMENTO:

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1

Objeto y ámbito de aplicación

El presente Reglamento establece el esquema europeo de certificación de la ciberseguridad basado en los criterios comunes (en lo sucesivo, «EUCC»).

El presente Reglamento se aplica a todos los productos de tecnologías de la información y la comunicación (en lo sucesivo, «TIC»), incluida su documentación, que se presenten para su certificación en virtud del EUCC, y a todos los perfiles de protección que se presenten para su certificación en el marco del proceso de TIC conducente a la certificación de productos de TIC.

Artículo 2

Definiciones

A efectos del presente Reglamento, se entenderá por:

1) «criterios comunes»: 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;

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;

3) «objeto de evaluación»: producto o parte de un producto de TIC, o perfil de protección dentro de un proceso de TIC, que se somete a una evaluación de ciberseguridad para obtener la certificación EUCC;

4) «declaración de seguridad»: alegación de requisitos de seguridad dependientes de la implementación con respecto a un determinado producto de TIC;

5) «perfil de protección»: proceso de TIC que establece los requisitos de seguridad para una categoría específica de productos de TIC, abordando necesidades de seguridad independientes de la implementación, y que puede utilizarse para evaluar productos de TIC pertenecientes a dicha categoría específica a efectos de su certificación;

6) «informe técnico de evaluación»: documento elaborado por una ITSEF para exponer las constataciones, opiniones y justificaciones obtenidas durante la evaluación de un producto de TIC o de un perfil de protección con arreglo a las normas y obligaciones establecidas en el presente Reglamento;

7) «ITSEF»: instalación de evaluación de la seguridad de las tecnologías de la información, que constituye un organismo de evaluación de la conformidad, según se define en el artículo 2, punto 13, del Reglamento (CE) n.º 765/2008, que desempeña actividades de evaluación;

8) «nivel AVA_VAN»: nivel de garantía de análisis de vulnerabilidades que indica el grado de actividades de evaluación de la ciberseguridad llevadas a cabo para determinar el nivel de resistencia ante el posible aprovechamiento de defectos o debilidades del objeto de evaluación en su entorno operativo, tal como se establece en los criterios comunes;

9) «certificado EUCC»: certificado de ciberseguridad expedido en virtud del EUCC a productos de TIC, o a perfiles de protección que puedan utilizarse exclusivamente en el proceso de certificación de productos de TIC;

10) «producto compuesto»: producto de TIC que se evalúa junto con otro producto de TIC subyacente que ya ha obtenido un certificado EUCC y de cuya funcionalidad de seguridad depende el producto de TIC compuesto;

11) «autoridad nacional de certificación de la ciberseguridad»: autoridad designada por un Estado miembro en virtud del artículo 58, apartado 1, del Reglamento (UE) 2019/881;

12) «organismo de certificación»: organismo de evaluación de la conformidad, según se define en el artículo 2, punto 13, del Reglamento (CE) n.º 765/2008, que desempeña actividades de certificación;

13) «ámbito técnico»: marco técnico común relacionado con una tecnología concreta para la certificación armonizada que presenta un conjunto de requisitos de seguridad característicos;

14) «documento del estado de la técnica»: documento que especifica los métodos, las técnicas y los instrumentos de evaluación aplicables a la certificación de productos de TIC o los requisitos de seguridad de una categoría genérica de productos de TIC, o cualquier otro requisito necesario para la certificación, con el fin de armonizar la evaluación, en concreto de los ámbitos técnicos o de los perfiles de protección;

15) «autoridad de vigilancia del mercado»: una autoridad según se define en el artículo 3, punto 4, del Reglamento (UE) 2019/1020.

Artículo 3

Normas de evaluación

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.

Artículo 4

Niveles de garantía

1. Los organismos de certificación expedirán certificados EUCC con nivel de garantía «sustancial» o «elevado».

2. Los certificados EUCC con nivel de garantía «sustancial» corresponderán a certificados que abarquen los niveles AVA_VAN 1 o 2.

3. Los certificados EUCC con nivel de garantía «elevado» corresponderán a certificados que abarquen los niveles AVA_VAN 3, 4 o 5.

4. El nivel de garantía confirmado en un certificado EUCC distinguirá entre el uso conforme y aumentado de los componentes de garantía, tal como se especifica en los criterios comunes y con arreglo a lo dispuesto en el anexo VIII.

5. Los organismos de evaluación de la conformidad aplicarán los componentes de garantía de los que dependa el nivel AVA_VAN seleccionado, con arreglo a lo dispuesto en las normas a que se refiere el artículo 3.

Artículo 5

Métodos de certificación de los productos de TIC

1. La certificación de un producto de TIC se llevará a cabo en función de su declaración de seguridad:

a) según la defina el solicitante, o

b) con la incorporación de 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. Los perfiles de protección se certificarán únicamente a efectos de la certificación de productos de TIC que pertenezcan a la categoría específica de productos de TIC cubierta por el perfil de protección.

Artículo 6

Autoevaluación de la conformidad

No se permitirá la autoevaluación de la conformidad en el sentido del artículo 53 del Reglamento (UE) 2019/881.

CAPÍTULO II

CERTIFICACIÓN DE PRODUCTOS DE TIC

Sección I

Normas y requisitos específicos para la evaluación

Artículo 7

Criterios y métodos de evaluación de los productos de TIC

1. Los productos de TIC que se presenten para su certificación se evaluarán, como mínimo, con arreglo a los siguientes aspectos:

a) los elementos aplicables de las normas a que se refiere el artículo 3;

b) las clases de requisitos de garantía de seguridad para la evaluación de vulnerabilidad y las pruebas funcionales independientes, según lo establecido en las normas de evaluación a que se refiere el artículo 3;

c) el nivel de riesgo asociado al uso previsto de los productos de TIC de que se trate de conformidad con el artículo 52 del Reglamento (UE) 2019/881 y sus funciones de seguridad que contribuyen a los objetivos de seguridad establecidos en el artículo 51 del citado Reglamento;

d) los documentos del estado de la técnica enumerados en el anexo I que resulten aplicables;

e) los perfiles de protección certificados enumerados en el anexo II que resulten aplicables.

2. En casos excepcionales y debidamente justificados, un organismo de evaluación de la conformidad podrá solicitar abstenerse de aplicar el documento del estado de la técnica pertinente. En tales casos, el organismo de evaluación de la conformidad informará a la autoridad nacional de certificación de la ciberseguridad incluyendo una justificación debidamente motivada de su solicitud. La autoridad nacional de certificación de la ciberseguridad evaluará si la excepción está justificada y, en caso de que así sea, la aprobará. Mientras esté pendiente la decisión de la autoridad nacional de

certificación de la ciberseguridad, el organismo de evaluación de la conformidad no expedirá ningún certificado. La autoridad nacional de certificación de la ciberseguridad notificará la excepción aprobada, sin demora indebida, al Grupo Europeo de Certificación de la Ciberseguridad, que podrá emitir un dictamen. La autoridad nacional de certificación de la ciberseguridad tendrá sumamente en cuenta el dictamen del Grupo Europeo de Certificación de la Ciberseguridad.

3. La certificación de los productos de TIC en los niveles AVA_VAN.4 o AVA_VAN.5 solo será posible en los siguientes supuestos:

a) cuando el producto de TIC esté contemplado en cualquiera de los ámbitos técnicos enumerados en el anexo I, se evaluará de conformidad con los documentos del estado de la técnica pertinentes de dichos ámbitos técnicos que resulten aplicables,

b) cuando el producto de TIC pertenezca a una categoría de productos de TIC cubiertos por un perfil de protección certificado que incluya los niveles AVA_VAN.4 o AVA_VAN.5 y que haya sido incluido como un perfil de protección del estado de la técnica en el anexo II, se evaluará de conformidad con la metodología de evaluación que se haya determinado para dicho perfil de protección,

c) cuando las letras a) y b) del presente apartado no resulten aplicables y sea poco probable la inclusión de un ámbito técnico en el anexo I o de un perfil de protección certificado en el anexo II en un futuro próximo, y solo en casos excepcionales debidamente justificados, con sujeción a las condiciones establecidas en el apartado 4.

4. Cuando un organismo de evaluación de la conformidad considere que se encuentra ante un caso excepcional y debidamente justificado a que se refiere el apartado 3, letra c), notificará la certificación prevista a la autoridad nacional de certificación de la ciberseguridad, junto con una justificación y una propuesta de metodología de evaluación. La autoridad nacional de certificación de la ciberseguridad evaluará si la excepción está justificada y, en caso de que así sea, aprobará o modificará la metodología de evaluación que deberá aplicar el organismo de evaluación de la conformidad. Mientras esté pendiente la decisión de la autoridad nacional de certificación de la ciberseguridad, el organismo de evaluación de la conformidad no expedirá ningún certificado. La autoridad nacional de certificación de la ciberseguridad informará, sin demora indebida, de la certificación prevista al Grupo Europeo de Certificación de la Ciberseguridad, que podrá emitir un dictamen. La autoridad nacional de certificación de la ciberseguridad tendrá sumamente en cuenta el dictamen del Grupo Europeo de Certificación de la Ciberseguridad.

5. En el caso de aquellos productos de TIC que se evalúen como producto compuesto de conformidad con los documentos del estado de la técnica pertinentes, la ITSEF que haya llevado a cabo la evaluación del producto de TIC subyacente compartirá la información pertinente con la ITSEF encargada de evaluar el producto de TIC compuesto.

Sección II

Expedición, renovación y retirada de certificados EUCC

Artículo 8

Información necesaria para la certificación

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.

2. La información a que se refiere el apartado 1 incluirá todas las pruebas pertinentes con arreglo a las secciones de «Elementos de acción del desarrollador» en el formato adecuado según lo establecido en las secciones de «Contenido y presentación de elementos de prueba» de los criterios comunes y la metodología común de evaluación para el nivel de garantía seleccionado y los requisitos de garantía de seguridad asociados. Las pruebas contendrán, en caso necesario, información sobre el producto de TIC y su código fuente de conformidad con el presente Reglamento, con sujeción a salvaguardias contra la divulgación no autorizada.

3. Los solicitantes de certificación podrán presentar al organismo de certificación y a la ITSEF resultados de evaluación adecuados de certificaciones anteriores en virtud:

a) del presente Reglamento;

b) de otro esquema europeo de certificación de la ciberseguridad adoptado de conformidad con el artículo 49 del Reglamento (UE) 2019/881;

c) de un esquema nacional a que se refiere el artículo 49 del presente Reglamento.

4. Cuando los resultados de la evaluación sean pertinentes para sus tareas, la ITSEF podrá reutilizar los resultados de evaluación siempre que estos se ajusten a los requisitos aplicables y se confirme su autenticidad.

5. Cuando el organismo de certificación permita que un producto se certifique como producto compuesto, el solicitante de la certificación pondrá a disposición de dicho organismo y de la ITSEF todos los elementos necesarios, en su caso, con arreglo al documento del estado de la técnica pertinente.

6. Los solicitantes de la certificación también proporcionarán al organismo de certificación y a la ITSEF la siguiente información:

a) el enlace a su sitio web que contenga la información complementaria sobre ciberseguridad a que se refiere el artículo 55 del Reglamento (UE) 2019/881;

b) una descripción de los procedimientos de gestión de vulnerabilidades y divulgación de vulnerabilidades del solicitante.

7. Toda la documentación pertinente a que se refiere el presente artículo será conservada por el organismo de certificación, la ITSEF y el solicitante durante un período de cinco años a partir de la expiración del certificado.

Artículo 9

Condiciones para la expedición de un certificado EUCC

1. Los organismos de certificación expedirán un certificado EUCC cuando se cumplan todas las condiciones siguientes:

a) la categoría de producto de TIC está comprendida en el ámbito de aplicación de la acreditación y, en su caso, de la autorización, del organismo de certificación y de la ITSEF intervinientes en la certificación;

b) el solicitante de la certificación ha firmado una declaración en la que contrae todos los compromisos enumerados en el apartado 2;

c) la ITSEF ha concluido la evaluación sin objeciones con arreglo a las normas, los criterios y los métodos de evaluación a que se refieren los artículos 3 y 7;

d) el organismo de certificación ha concluido la revisión de los resultados de la evaluación sin objeciones;

e) el organismo de certificación ha verificado que los informes técnicos de evaluación presentados por la ITSEF son coherentes con las pruebas aportadas y que se han aplicado correctamente las normas, los criterios y los métodos de evaluación a que se refieren los artículos 3 y 7.

2. El solicitante de la certificación contraerá los siguientes compromisos:

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;

b) abstenerse de promocionar el producto de TIC como certificado conforme al EUCC antes de que se haya expedido el certificado correspondiente;

c) promocionar la certificación del producto de TIC únicamente con respecto al ámbito de aplicación establecido en el certificado EUCC;

d) dejar inmediatamente de promocionar la certificación del producto de TIC en caso de suspensión, retirada o expiración del certificado EUCC;

e) garantizar que los productos de TIC comercializados con referencia al certificado EUCC sean estrictamente idénticos al producto de TIC sujeto a la certificación;

f) respetar las normas de uso de la marca y la etiqueta establecidas para el certificado EUCC de conformidad con el artículo 11.

3. En el caso de aquellos productos de TIC que se certifiquen como producto compuesto de conformidad con los documentos del estado de la técnica pertinentes, el organismo de certificación que haya certificado el producto de TIC subyacente compartirá la información pertinente con el organismo de certificación encargado de certificar el producto de TIC compuesto.

Artículo 10

Contenido y formato de los certificados EUCC

1. Los certificados EUCC incluirán, como mínimo, la información prevista en el anexo VII.

2. El ámbito de aplicación y los límites del producto de TIC certificado se especificarán de forma inequívoca en el certificado EUCC o en el informe de certificación, indicando si el producto de TIC ha sido certificado en su totalidad o solo parcialmente.

3. El organismo de certificación proporcionará al solicitante el certificado EUCC, como mínimo, en formato electrónico.

4. El organismo de certificación elaborará un informe de certificación de conformidad con el anexo V para cada certificado EUCC que expida. Dicho informe se basará en el informe técnico de evaluación presentado por la ITSEF. El informe técnico de evaluación y el informe de certificación indicarán los criterios y métodos de evaluación específicos a que se refiere el artículo 7 que se hayan utilizado en la evaluación.

5. El organismo de certificación facilitará a la autoridad nacional de certificación de la ciberseguridad y a ENISA todos los certificados EUCC y todos los informes de certificación en formato electrónico.

Artículo 11

Marca y etiqueta

1. El titular de un certificado podrá colocar una marca y una etiqueta en el producto de TIC certificado. La marca y la etiqueta demuestran que el producto de TIC ha sido certificado de conformidad con el presente Reglamento. Estos elementos se colocarán con arreglo a lo dispuesto en el presente artículo y en el anexo IX.

2. La marca y la etiqueta se colocarán en el producto de TIC certificado o en su placa descriptiva de manera visible, legible e indeleble. Cuando esto no sea posible o no pueda garantizarse debido a la naturaleza del producto, se colocará en el embalaje y en los documentos adjuntos. Cuando el producto de TIC certificado se entregue en forma de programa informático, la marca y la etiqueta figurarán de forma visible, legible e indeleble en la documentación adjunta, o esta documentación se pondrá a disposición de los usuarios de forma fácil y directa en un sitio web.

3. La marca y la etiqueta figurarán en el anexo IX e incluirán:

a) el nivel de garantía y el nivel AVA_VAN del producto de TIC certificado;

b) la identificación única del certificado, consistente en:

   1) el nombre del esquema;

   2) el nombre y el número de referencia de la acreditación del organismo de certificación que haya expedido el certificado;

   3) el año y el mes de emisión;

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

4. La marca y la etiqueta irán acompañadas de un código QR con un enlace a un sitio web que contenga, como mínimo:

a) la información sobre la validez del certificado;

b) la información necesaria sobre la certificación, con arreglo a lo dispuesto en los anexos V y VII;

c) la información que el titular del certificado debe poner a disposición del público de conformidad con el artículo 55 del Reglamento (UE) 2019/881;

d) cuando proceda, la información histórica relacionada con la certificación o certificaciones específicas del producto de TIC para permitir la trazabilidad.

Artículo 12

Período de validez de un certificado EUCC

1. El organismo de certificación establecerá un período de validez para cada certificado EUCC expedido teniendo en cuenta las características del producto de TIC certificado.

2. El período máximo de validez de un certificado EUCC será de cinco años.

3. No obstante lo dispuesto en el apartado 2, se podrá establecer un período superior a cinco años, previa aprobación de la autoridad nacional de certificación de la ciberseguridad, que deberá notificar sin demora indebida al Grupo Europeo de Certificación de la Ciberseguridad la aprobación otorgada.

Artículo 13

Revisión de un certificado EUCC

1. A petición del titular del certificado o por otros motivos justificados, el organismo de certificación podrá decidir revisar el certificado EUCC de un producto de TIC. 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 producto de TIC certificado.

2. A partir de los resultados de la revisión y, en su caso, de la revaluación, el organismo de certificación:

a) confirmará el certificado EUCC;

b) retirará el certificado EUCC de conformidad con el artículo 14;

c) retirará el certificado EUCC de conformidad con el artículo 14 y expedirá un nuevo certificado EUCC con un ámbito de aplicación idéntico y un período de validez ampliado; o

d) retirará el certificado EUCC de conformidad con el artículo 14 y expedirá un nuevo certificado EUCC con un ámbito de aplicación diferente.

3. El organismo de certificación podrá decidir suspender, sin demora indebida, el certificado EUCC de conformidad con el artículo 30, en espera de la adopción de medidas correctoras por parte del titular del citado certificado.

Artículo 14

Retirada de un certificado EUCC

1. Sin perjuicio de lo dispuesto en el artículo 58, apartado 8, letra e), del Reglamento (UE) 2019/881, un certificado EUCC podrá ser retirado por el organismo de certificación que lo expidió.

2. El organismo de certificación a que se refiere el apartado 1 notificará la retirada del certificado a la autoridad nacional de certificación de la ciberseguridad. Asimismo, notificará la retirada a ENISA con el fin de facilitar el desempeño de su cometido en virtud del artículo 50 del Reglamento (UE) 2019/881. Por su parte, la autoridad nacional de certificación de la ciberseguridad informará al respecto a las demás autoridades de vigilancia del mercado pertinentes.

3. El titular de un certificado EUCC podrá solicitar la retirada de dicho certificado.

CAPÍTULO III

CERTIFICACIÓN DE PERFILES DE PROTECCIÓN

Sección I

Normas y requisitos específicos para la evaluación

Artículo 15

Criterios y métodos de evaluación

1. Los perfiles de protección se evaluarán, como mínimo, con arreglo a los siguientes aspectos:

a) los elementos aplicables de las normas a que se refiere el artículo 3;

b) el nivel de riesgo asociado al uso previsto de los productos de TIC de que se trate de conformidad con el artículo 52 del Reglamento (UE) 2019/881 y sus funciones de seguridad que contribuyen a los objetivos de seguridad establecidos en el artículo 51 de dicho Reglamento;

c) los documentos del estado de la técnica enumerados en el anexo I que resulten aplicables. Los perfiles de protección contemplados en un ámbito técnico se certificarán con arreglo a los requisitos establecidos en dicho ámbito técnico.

2. En casos excepcionales y debidamente justificados, un organismo de evaluación de la conformidad podrá certificar un perfil de protección sin aplicar los documentos del estado de la técnica pertinentes. En tales casos, informará a la autoridad nacional de certificación competente de la ciberseguridad y justificará la certificación prevista sin aplicar los documentos del estado de la técnica pertinentes, así como la metodología de evaluación propuesta. La autoridad nacional de certificación de la ciberseguridad evaluará si la certificación está justificada y, en caso de que así sea, aprobará que no se apliquen los documentos del estado de la técnica pertinentes y aprobará o modificará, cuando proceda, la metodología de evaluación que deberá aplicar el organismo de evaluación de la conformidad. Mientras esté pendiente la decisión de la autoridad nacional de certificación de la ciberseguridad, el organismo de evaluación de la conformidad no expedirá ningún certificado para el perfil de protección. La autoridad nacional de certificación de la ciberseguridad notificará, sin demora indebida, la autorización de la no aplicación de los documentos del estado de la técnica pertinentes al Grupo Europeo de Certificación de la Ciberseguridad, que podrá emitir un dictamen. La autoridad nacional de certificación de la ciberseguridad tendrá sumamente en cuenta el dictamen del Grupo Europeo de Certificación de la Ciberseguridad.

Sección II

Expedición, renovación y retirada de certificados EUCC relativos a perfiles de protección

Artículo 16

Información necesaria para la certificación 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. El artículo 8, apartados 2, 3, 4 y 7, se aplicará *mutatis mutandis*.

Artículo 17

Expedición de certificados EUCC para perfiles de protección

1. El solicitante de la certificación proporcionará al organismo de certificación y a la ITSEF toda la información necesaria, completa y correcta.

2. Los artículos 9 y 10 se aplicarán *mutatis mutandis*.

3. La ITSEF evaluará si un perfil de protección es completo, coherente, sólido desde el punto de vista técnico y eficaz para el uso previsto y con respecto a los objetivos de seguridad de la categoría de productos de TIC cubierta por dicho perfil de protección.

4. Los perfiles de protección solo los certificará:

a) una autoridad nacional de certificación de la ciberseguridad u otro organismo público acreditado como organismo de certificación; o

b) un organismo de certificación, previa aprobación por parte de la autoridad nacional de certificación de la ciberseguridad de cada perfil de protección individual.

Artículo 18

Período de validez de los certificados EUCC relativos a perfiles de protección

1. El organismo de certificación establecerá un período de validez para cada certificado EUCC.

2. Dicho período de validez será, como máximo, equivalente a la duración del perfil de protección de que se trate.

Artículo 19

Revisión de los certificados EUCC relativos a perfiles de protección

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 con arreglo a las condiciones establecidas en el artículo 15. 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.

2. A partir de los resultados de la revisión y, en su caso, de la revaluación, el organismo de certificación adoptará una de las siguientes medidas:

a) confirmará el certificado EUCC;

b) retirará el certificado EUCC de conformidad con el artículo 20;

c) retirará el certificado EUCC de conformidad con el artículo 20 y expedirá un nuevo certificado EUCC con un ámbito de aplicación idéntico y un período de validez ampliado;

d) retirará el certificado EUCC de conformidad con el artículo 20 y expedirá un nuevo certificado EUCC con un ámbito de aplicación diferente.

Artículo 20

Retirada de un certificado EUCC relativo a un perfil de protección

1. Sin perjuicio de lo dispuesto en el artículo 58, apartado 8, letra e), del Reglamento (UE) 2019/881, un certificado EUCC relativo a un perfil de protección podrá ser retirado por el organismo de certificación que lo expidió. El artículo 14 se aplicará *mutatis mutandis*.

2. La autoridad nacional de certificación de la ciberseguridad que haya aprobado dicho certificado retirará los certificados de perfil de protección expedidos de conformidad con el artículo 17, apartado 4, letra b).

CAPÍTULO IV

Organismos de evaluación de la conformidad

Artículo 21

Requisitos adicionales o específicos aplicables a los organismos de certificación

1. La autoridad nacional de certificación de la ciberseguridad autorizará a un organismo de certificación a expedir certificados EUCC con un nivel de garantía «elevado» cuando dicho organismo demuestre que, además de reunir los requisitos previstos en el artículo 60, apartado 1, y en el anexo del Reglamento (UE) 2019/881 por lo que respecta a la acreditación de organismos de evaluación de la conformidad, cumple las siguientes condiciones:

a) posee los conocimientos especializados y las competencias necesarios para tomar una decisión de certificación con nivel de garantía «elevado»;

b) desarrolla sus actividades de certificación en cooperación con una ITSEF autorizada de conformidad con el artículo 22;

c) dispone de las competencias necesarias y ha adoptado medidas técnicas y operativas adecuadas para proteger eficazmente la información confidencial y delicada con nivel de garantía «elevado», además de los requisitos establecidos en el artículo 43.

2. La autoridad nacional de certificación de la ciberseguridad determinará si un organismo de certificación cumple todos los requisitos previstos en el apartado 1. A tal efecto, deberá llevar a cabo, como mínimo, entrevistas estructuradas y una revisión de al menos una certificación piloto realizada por el organismo de certificación de conformidad con el presente Reglamento.

En su evaluación, la autoridad nacional de certificación de la ciberseguridad podrá reutilizar cualquier prueba adecuada que proceda de una autorización previa o de actividades similares concedidas en virtud:

a) del presente Reglamento;

b) de otro esquema europeo de certificación de la ciberseguridad adoptado de conformidad con el artículo 49 del Reglamento (UE) 2019/881;

c) de un esquema nacional a que se refiere el artículo 49 del presente Reglamento.

3. La autoridad nacional de certificación de la ciberseguridad elaborará un informe de autorización, que será objeto de una revisión por pares de conformidad con el artículo 59, apartado 3, letra d), del Reglamento (UE) 2019/881.

4. La autoridad nacional de certificación de la ciberseguridad especificará las categorías de productos de TIC y los perfiles de protección sobre los que se extiende la autorización, cuyo período de validez no podrá ser superior al período de validez de la acreditación. La autorización podrá renovarse previa solicitud, siempre que el organismo de certificación siga reuniendo los requisitos establecidos en el presente artículo. Para la renovación de la autorización, no se exigen evaluaciones piloto.

5. La autoridad nacional de certificación de la ciberseguridad retirará la autorización del organismo de certificación en caso de que este deje de cumplir las condiciones establecidas en el presente artículo. Tras la retirada de la autorización, el organismo de certificación dejará inmediatamente de promocionarse como organismo de certificación autorizado.

Artículo 22

Requisitos adicionales o específicos aplicables a las ITSEF

1. La autoridad nacional de certificación de la ciberseguridad autorizará a una ITSEF a llevar a cabo la evaluación de productos de TIC sujetos a certificación con un nivel de garantía «elevado» cuando dicha ITSEF demuestre que, además de reunir los requisitos previstos en el artículo 60, apartado 1, y en el anexo del Reglamento (UE) 2019/881 por lo que respecta a la acreditación de organismos de evaluación de la conformidad, cumple todas las condiciones siguientes:

a) posee los conocimientos especializados necesarios para desempeñar las actividades de evaluación al objeto de determinar la resistencia a los ciberataques de última generación llevados a cabo por agentes con capacidades y recursos significativos;

b) con respecto a los ámbitos técnicos y los perfiles de protección, que forman parte del proceso de TIC para esos productos de TIC:

1) posee los conocimientos especializados necesarios para desempeñar las actividades de evaluación específicas necesarias para determinar metódicamente la resistencia de un objeto de evaluación frente a atacantes expertos en su entorno operativo, suponiendo un potencial de ataque «moderado» o «alto» con arreglo a lo dispuesto en las normas a que se refiere el artículo 3;

2) dispone de las competencias técnicas especificadas en los documentos del estado de la técnica enumerados en el anexo I;

c) dispone de las competencias necesarias y ha adoptado medidas técnicas y operativas adecuadas para proteger eficazmente la información confidencial y delicada con nivel de garantía «elevado», además de los requisitos establecidos en el artículo 43.

2. La autoridad nacional de certificación de la ciberseguridad determinará si una ITSEF cumple todos los requisitos previstos en el apartado 1. A tal efecto, deberá llevar a cabo, como mínimo, entrevistas estructuradas y una revisión de al menos una evaluación piloto realizada por la ITSEF de conformidad con el presente Reglamento.

3. En su evaluación, la autoridad nacional de certificación de la ciberseguridad podrá reutilizar cualquier prueba adecuada que proceda de una autorización previa o de actividades similares concedidas en virtud:

a) del presente Reglamento;

b) de otro esquema europeo de certificación de la ciberseguridad adoptado de conformidad con el artículo 49 del Reglamento (UE) 2019/881;

c) de un esquema nacional a que se refiere el artículo 49 del presente Reglamento.

4. La autoridad nacional de certificación de la ciberseguridad elaborará un informe de autorización, que será objeto de una revisión por pares de conformidad con el artículo 59, apartado 3, letra d), del Reglamento (UE) 2019/881.

5. La autoridad nacional de certificación de la ciberseguridad especificará las categorías de productos de TIC y los perfiles de protección sobre los que se extiende la autorización, cuyo período de validez no podrá ser superior al período de validez de la acreditación. La autorización podrá renovarse previa solicitud, siempre que la ITSEF siga reuniendo los requisitos establecidos en el presente artículo. Para la renovación de la autorización, no deben exigirse evaluaciones piloto.

6. La autoridad nacional de certificación de la ciberseguridad retirará la autorización de la ITSEF en caso de que esta deje de cumplir las condiciones establecidas en el presente artículo. Tras la retirada de la autorización, la ITSEF dejará de promocionarse como ITSEF autorizada.

Artículo 23

Notificación de organismos de certificación

1. La autoridad nacional de certificación de la ciberseguridad notificará a la Comisión los organismos de certificación de su territorio que sean competentes para expedir certificaciones con nivel de garantía «sustancial» en virtud de su acreditación.

2. Asimismo, la autoridad nacional de certificación de la ciberseguridad notificará a la Comisión los organismos de certificación de su territorio que sean competentes para expedir certificaciones con nivel de garantía «elevado» en virtud de su acreditación y de la decisión de autorización.

3. La autoridad nacional de certificación de la ciberseguridad proporcionará, como mínimo, la siguiente información cuando notifique organismos de certificación a la Comisión:

a) el nivel o niveles de garantía con los que el organismo de certificación puede expedir certificados EUCC con arreglo a sus competencias;

b) la siguiente información relacionada con la acreditación:

1) fecha de la acreditación;

2) nombre y dirección del organismo de certificación;

3) país de registro del organismo de certificación;

4) número de referencia de la acreditación;

5) alcance y duración de la validez de la acreditación;

6) la dirección, la ubicación y el enlace al sitio web pertinente del organismo nacional de acreditación;

c) la siguiente información relativa a la autorización de nivel «elevado»:

1) fecha de la autorización;

2) número de referencia de la autorización;

3) duración de la validez de la autorización;

4) ámbito de la autorización, incluido el nivel AVA_VAN más elevado y, en su caso, el ámbito técnico cubierto.

4. La autoridad nacional de certificación de la ciberseguridad enviará una copia de la notificación a que se refieren los apartados 1 y 2 a ENISA para la publicación de información precisa en el sitio web de certificación de la ciberseguridad en relación con la admisibilidad de los organismos de certificación.

5. La autoridad nacional de certificación de la ciberseguridad examinará sin demora indebida toda información sobre cualquier cambio en el estado de la acreditación facilitada por el organismo nacional de acreditación. En caso de retirada de la acreditación o la autorización, la autoridad nacional de certificación de la ciberseguridad informará de ello a la Comisión y podrá presentarle una solicitud en virtud del artículo 61, apartado 4, del Reglamento (UE) 2019/881.

Artículo 24

Notificación de ITSEF

Las obligaciones de notificación de las autoridades nacionales de certificación de la ciberseguridad establecidas en el artículo 23 también se aplicarán a las ITSEF. La notificación incluirá la dirección de la ITSEF, la acreditación válida y, en su caso, la autorización válida de dicho organismo.

CAPÍTULO V

CONTROL, FALTA DE CONFORMIDAD E INCUMPLIMIENTO

Sección I

CONTROL DEL CUMPLIMIENTO

Artículo 25

Actividades de control por parte de la autoridad nacional de certificación de la ciberseguridad

1. Sin perjuicio de lo dispuesto en el artículo 58, apartado 7, del Reglamento (UE) 2019/881, la autoridad nacional de certificación de la ciberseguridad controlará el cumplimiento:

a) del organismo de certificación y la ITSEF con las obligaciones que les incumben en virtud del presente Reglamento y del Reglamento (UE) 2019/881;

b) de los titulares de certificados EUCC con las obligaciones que les incumben en virtud del presente Reglamento y del Reglamento (UE) 2019/881;

c) de los productos de TIC certificados con los requisitos establecidos en el EUCC;

d) de la garantía indicada en el certificado EUCC para abordar la evolución del panorama de amenazas.

2. La autoridad nacional de certificación de la ciberseguridad llevará a cabo sus actividades de control basándose en particular en:

a) la información procedente de los organismos de certificación, los organismos nacionales de acreditación y las autoridades de vigilancia del mercado pertinentes;

b) la información resultante de las auditorías e investigaciones realizadas por ella misma o por otra autoridad;

c) el muestreo llevado a cabo de conformidad con el apartado 3;

d) las reclamaciones recibidas.

3. La autoridad nacional de certificación de la ciberseguridad, en cooperación con otras autoridades de vigilancia del mercado, muestreará anualmente, como mínimo, el 4 % de los certificados EUCC, según determine una evaluación de riesgos. Previa solicitud y actuando en nombre de la autoridad nacional de certificación de la ciberseguridad competente, los organismos de certificación y, en caso necesario, la ITSEF asistirán a dicha autoridad en el control del cumplimiento.

4. La autoridad nacional de certificación de la ciberseguridad seleccionará la muestra de productos de TIC certificados que se inspeccionarán en función de criterios objetivos, entre ellos:

a) la categoría de producto;

b) los niveles de garantía de los productos;

c) el titular de un certificado;

d) el organismo de certificación y, en su caso, la ITSEF subcontratada;

e) cualquier otra información puesta en conocimiento de la autoridad.

5. La autoridad nacional de certificación de la ciberseguridad informará a los titulares de certificados EUCC acerca de los productos de TIC seleccionados y los criterios de selección.

6. El organismo de certificación que haya certificado el producto de TIC muestreado, previa solicitud de la autoridad nacional de certificación de la ciberseguridad, con la asistencia de la respectiva ITSEF, llevará a cabo una revisión adicional con arreglo al procedimiento establecido en el anexo IV, sección IV.2, e informará de los resultados a la autoridad nacional de certificación de la ciberseguridad.

7. Cuando la autoridad nacional de certificación de la ciberseguridad tenga motivos suficientes para creer que un producto de TIC certificado ya no cumple el presente Reglamento o el Reglamento (UE) 2019/881, podrá llevar a cabo investigaciones o ejercer cualquier otra competencia de control prevista en el artículo 58, apartado 8, del Reglamento (UE) 2019/881.

8. La autoridad nacional de certificación de la ciberseguridad informará al organismo de certificación y a la ITSEF correspondientes de las investigaciones en curso relativas a los productos de TIC seleccionados.

9. Cuando la autoridad nacional de certificación de la ciberseguridad constate que una investigación en curso se refiere a productos de TIC certificados por organismos de certificación establecidos en otros Estados miembros, informará de ello a las autoridades nacionales de certificación de la ciberseguridad de los Estados miembros pertinentes con el fin de colaborar en las investigaciones, cuando proceda. Asimismo, dicha autoridad nacional de certificación de la ciberseguridad deberá notificar al Grupo Europeo de Certificación de la Ciberseguridad la realización de investigaciones transfronterizas y los resultados subsiguientes.

Artículo 26

Actividades de control por parte del organismo de certificación

1. El organismo de certificación controlará:

a) el cumplimiento de los titulares de certificados con las obligaciones que les incumben en virtud del presente Reglamento y del Reglamento (UE) 2019/881 en relación con los certificados EUCC expedidos por el organismo de certificación;

b) el cumplimiento de los productos de TIC que haya certificado con sus respectivos requisitos de seguridad;

c) la garantía indicada en los perfiles de protección certificados.

2. El organismo de certificación llevará a cabo sus actividades de control basándose en:

a) la información facilitada en virtud de los compromisos del solicitante de la certificación a que se refiere el artículo 9, apartado 2;

b) la información resultante de las actividades de otras autoridades de vigilancia del mercado pertinentes;

c) las reclamaciones recibidas;

d) la información de vulnerabilidad que pueda afectar a los productos de TIC que haya certificado.

3. La autoridad nacional de certificación de la ciberseguridad podrá elaborar normas sobre un diálogo periódico entre los organismos de certificación y los titulares de certificados EUCC al objeto de verificar el cumplimiento de los compromisos contraídos en virtud del artículo 9, apartado 2, e informar sobre dicho cumplimiento, sin perjuicio de las actividades relacionadas con otras autoridades de vigilancia del mercado pertinentes.

Artículo 27

Actividades de control por parte de los titulares de certificados

1. Los titulares de certificados EUCC llevarán a cabo las siguientes tareas para controlar la conformidad del producto de TIC certificado con sus requisitos de seguridad:

a) control de la información de vulnerabilidad relativa al producto de TIC certificado, incluidas las dependencias conocidas por sus propios medios, pero también teniendo en cuenta:

   1) la publicación o presentación de información sobre vulnerabilidad por parte de un usuario o un investigador en materia de seguridad a que se refiere el artículo 55, apartado 1, letra c), del Reglamento (UE) 2019/881;

   2) la presentación de información por cualquier otra fuente;

b) control de la garantía indicada en el certificado EUCC.

2. Los titulares de certificados EUCC trabajarán en cooperación con el organismo de certificación, la ITSEF y, en su caso, la autoridad nacional de certificación de la ciberseguridad, para apoyar sus actividades de control.

Sección II

CONFORMIDAD Y CUMPLIMIENTO

Artículo 28

Consecuencias de la falta de conformidad de un producto de TIC certificado o de un perfil de protección

1. Cuando un producto de TIC certificado o un perfil de protección no sean conformes con los requisitos establecidos en el presente Reglamento y en el Reglamento (UE) 2019/881, el organismo de certificación informará al titular del certificado EUCC sobre la falta de conformidad detectada y solicitará medidas correctoras al respecto.

2. En el supuesto de que una falta de conformidad con las disposiciones del presente Reglamento pueda afectar al cumplimiento de otra legislación pertinente de la Unión que prevea la posibilidad de demostrar la presunción de conformidad con los requisitos de dicho acto jurídico mediante el certificado EUCC, el organismo de certificación informará sin demora a la autoridad nacional de certificación de la ciberseguridad, que notificará de inmediato la falta de conformidad detectada a la autoridad de vigilancia del mercado competente en relación con esa otra legislación pertinente de la Unión.

3. Una vez recibida la información a que se refiere el apartado 1, el titular del certificado EUCC propondrá al organismo de certificación, dentro del plazo fijado por este, que no será superior a treinta días, las medidas correctoras necesarias para subsanar la falta de conformidad.

4. El organismo de certificación podrá suspender, sin demora indebida, el certificado EUCC en virtud del artículo 30 en caso de emergencia o cuando su titular no coopere adecuadamente con el organismo de certificación.

5. El organismo de certificación llevará a cabo una revisión en virtud de los artículos 13 y 19 con el fin de determinar si las medidas correctoras subsanan la falta de conformidad.

6. Cuando el titular del certificado EUCC no proponga medidas correctoras adecuadas durante el período a que se refiere el apartado 3, se procederá a suspender el certificado de conformidad con el artículo 30 o a retirarlo de conformidad con los artículos 14 o 20.

7. El presente artículo no se aplicará a los casos de vulnerabilidades que afecten a un producto de TIC certificado, que se tratarán con arreglo a lo dispuesto en el capítulo VI.

Artículo 29

Consecuencias del incumplimiento por parte del titular de un certificado

1. Cuando el organismo de certificación constate que:

a) el titular de un certificado EUCC o el solicitante de una certificación no cumplen los compromisos y obligaciones que les incumben en virtud del artículo 9, apartado 2, el artículo 17, apartado 2, y los artículos 27 y 41; o que

b) el titular de un certificado EUCC no cumple lo dispuesto en el artículo 56, apartado 8, del Reglamento (UE) 2019/881 o en el capítulo VI del presente Reglamento;

fijará un plazo no superior a treinta días para que dicho titular adopte medidas correctoras.

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 y artículo 20.

3. La infracción continuada o recurrente por parte del titular de un certificado EUCC de las obligaciones que le incumben en virtud del apartado 1 dará lugar a la retirada de dicho certificado de conformidad con los artículos 14 o 20.

4. El organismo de certificación informará a la autoridad nacional de certificación de la ciberseguridad de las constataciones a que se refiere el apartado 1. Cuando el caso de incumplimiento afecte al cumplimiento de otra legislación pertinente de la Unión, la autoridad nacional de certificación de la ciberseguridad notificará de inmediato el caso de incumplimiento detectado a la autoridad de vigilancia del mercado competente en relación con esa otra legislación pertinente de la Unión.

Artículo 30

Suspensión de un certificado EUCC

1. Cuando el presente Reglamento se refiera a la suspensión de un certificado EUCC, el organismo de certificación procederá a suspender dicho certificado durante un período adecuado a las circunstancias que hayan dado lugar a la suspensión, que no será superior a cuarenta y dos días. El período de suspensión comenzará al día siguiente de la decisión del organismo de certificación. La suspensión no afectará a la validez del certificado.

2. El organismo de certificación notificará la suspensión al titular del certificado y a la autoridad nacional de certificación de la ciberseguridad sin demora indebida y expondrá los motivos de su decisión, las medidas solicitadas que deben adoptarse y el período de suspensión.

3. Los titulares de la certificación comunicarán a los compradores de los productos de TIC afectados la suspensión y los motivos aducidos al respecto por el organismo de certificación, excepto aquellas partes de los motivos que contengan información delicada o cuya divulgación suponga un riesgo para la seguridad. El titular del certificado también pondrá esta información a disposición del público.

4. Cuando otra legislación pertinente de la Unión establezca una presunción de conformidad basada en los certificados expedidos en virtud de las disposiciones del presente Reglamento, la autoridad nacional de certificación de la ciberseguridad informará de la suspensión a la autoridad de vigilancia del mercado competente en relación con esa otra legislación pertinente de la Unión.

5. La suspensión de un certificado se notificará a ENISA de conformidad con el artículo 42, apartado 3.

6. En casos debidamente justificados, la autoridad nacional de certificación de la ciberseguridad podrá autorizar una prórroga del período de suspensión de un certificado EUCC. El período total de suspensión no podrá ser superior a un año.

Artículo 31

Consecuencias del incumplimiento por parte del organismo de evaluación de la conformidad

1. Cuando un organismo de certificación incumpla sus obligaciones, o el organismo de certificación pertinente detecte un incumplimiento por parte de una ITSEF, la autoridad nacional de certificación de la ciberseguridad deberá, sin demora indebida:

a) determinar, con la ayuda de la ITSEF interesada, los certificados EUCC potencialmente afectados;

b) en caso necesario, solicitar que se lleven a cabo actividades de evaluación de uno o varios productos de TIC o perfiles de protección, bien por parte de la ITSEF que realizó la evaluación, bien por cualquier otra ITSEF acreditada y, en su caso, autorizada, que pueda estar en mejores condiciones técnicas para contribuir a dicha determinación;

c) analizar los efectos del incumplimiento;

d) notificar el incumplimiento al titular del certificado EUCC afectado.

2. A partir de las medidas a que se refiere el apartado 1, el organismo de certificación adoptará una de las siguientes decisiones con respecto a cada certificado EUCC afectado:

a) mantener el certificado EUCC inalterado;

b) retirar el certificado EUCC de conformidad con el artículo 14 o artículo 20 y, en su caso, expedir un nuevo certificado EUCC.

3. Asimismo, a partir de las medidas a que se refiere el apartado 1, la autoridad nacional de certificación de la ciberseguridad deberá:

a) en caso necesario, informar al organismo nacional de acreditación del incumplimiento por parte del organismo de certificación o su respectiva ITSEF;

b) cuando proceda, determinar las posibles repercusiones en la autorización.

CAPÍTULO VI

GESTIÓN Y DIVULGACIÓN DE VULNERABILIDADES

Artículo 32

Ámbito de aplicación de la gestión de vulnerabilidades

El presente capítulo se aplica a los productos de TIC para los que se haya expedido un certificado EUCC.

Sección I

GESTIÓN DE VULNERABILIDADES

Artículo 33

Procedimientos de gestión de vulnerabilidades

1. El titular de un certificado EUCC establecerá y mantendrá todos los procedimientos necesarios de gestión de vulnerabilidades con arreglo a las normas previstas en la presente sección y, en su caso, complementados por los procedimientos establecidos en la norma EN ISO/IEC 30111.

2. El titular de un certificado EUCC mantendrá y publicará métodos adecuados para recibir información sobre vulnerabilidades relacionadas con sus productos de fuentes externas, en particular de usuarios, organismos de certificación e investigadores en materia de seguridad.

3. Cuando un titular de un certificado EUCC detecte o reciba información sobre una posible vulnerabilidad que afecte a un producto de TIC certificado, la registrará y llevará a cabo un análisis del impacto de la vulnerabilidad.

4. Cuando una posible vulnerabilidad afecte a un producto compuesto, el titular del certificado EUCC informará de esa posible vulnerabilidad al titular de los certificados EUCC dependientes.

5. En respuesta a una solicitud razonable por parte del organismo de certificación que haya expedido el certificado, el titular de un certificado EUCC le transmitirá toda la información pertinente sobre posibles vulnerabilidades.

Artículo 34

Evaluación de impacto de la vulnerabilidad

1. El análisis del impacto de la vulnerabilidad se referirá al objetivo de la evaluación y a las declaraciones de garantía contenidas en el certificado. El análisis del impacto de la vulnerabilidad se llevará a cabo en un plazo adecuado en función de en qué medida es aprovechable y grave la posible vulnerabilidad del producto de TIC certificado.

2. Cuando proceda, se calculará el potencial de ataque con arreglo a la metodología pertinente prevista en las normas a que se refiere el artículo 3 y los documentos del estado de la técnica pertinentes enumerados en el anexo I, con el fin de determinar en qué medida es aprovechable la vulnerabilidad. A tal efecto, se tendrá en cuenta el nivel AVA_VAN del certificado EUCC.

Artículo 35

Informe de la evaluación de impacto de la vulnerabilidad

1. El titular elaborará un informe del análisis del impacto de la vulnerabilidad cuando en este se revele que la vulnerabilidad puede repercutir en la conformidad del producto de TIC con su certificado.

2. El informe de la evaluación de impacto de la vulnerabilidad contendrá un análisis de los siguientes elementos:

a) el impacto de la vulnerabilidad en el producto de TIC certificado;

b) los posibles riesgos asociados a la proximidad o disponibilidad de un ataque;

c) si es posible subsanar la vulnerabilidad;

d) en caso de que pueda subsanarse la vulnerabilidad, las posibles resoluciones al respecto.

3. El informe de la evaluación de impacto de la vulnerabilidad contendrá, en su caso, información sobre las maneras en que puede aprovecharse la vulnerabilidad. Dicha información se tratará con arreglo a las medidas de seguridad adecuadas para proteger su confidencialidad y garantizar, en caso necesario, su limitada difusión.

4. El titular del certificado EUCC transmitirá sin demora indebida un informe del análisis del impacto de la vulnerabilidad al organismo de certificación o a la autoridad nacional de certificación de la ciberseguridad de conformidad con el artículo 56, apartado 8, del Reglamento (UE) 2019/881.

5. Si el informe del análisis del impacto de la vulnerabilidad determina que la vulnerabilidad no es residual en el sentido de las normas a las que se refiere el artículo 3 y que puede subsanarse, se aplicará el artículo 36.

6. Si el informe del análisis del impacto de la vulnerabilidad aprobado por el organismo de certificación determina que no puede subsanarse la vulnerabilidad, se procederá a retirar el certificado EUCC de conformidad con el artículo 14.

7. El titular del certificado EUCC supervisará cualquier vulnerabilidad residual para garantizar que no pueda aprovecharse en caso de que se produzcan cambios en el entorno operativo.

Artículo 36

Subsanación de vulnerabilidades

El titular de un certificado EUCC presentará al organismo de certificación una propuesta de medidas correctoras adecuadas. El organismo de certificación revisará el certificado de conformidad con el artículo 13. El alcance de dicha revisión vendrá determinado por la medida de subsanación de la vulnerabilidad que se haya propuesto.

Sección II

DIVULGACIÓN DE VULNERABILIDADES

Artículo 37

Información facilitada a la autoridad nacional de certificación de la ciberseguridad

1. La información facilitada por el organismo de certificación a la autoridad nacional de certificación de la ciberseguridad incluirá todos los elementos necesarios para que la autoridad nacional de certificación de la ciberseguridad conozca el impacto de la vulnerabilidad, las modificaciones que deben introducirse en el producto de TIC y, en su caso, cualquier información del organismo de certificación sobre las repercusiones más amplias que la vulnerabilidad puede tener en otros productos de TIC certificados.

2. La información facilitada en virtud del apartado 1 no contendrá datos sobre las maneras de aprovechar la vulnerabilidad. Esta disposición se entiende sin perjuicio de las competencias de investigación de la autoridad nacional de certificación de la ciberseguridad.

Artículo 38

Cooperación con otras autoridades nacionales de certificación de la ciberseguridad

1. La autoridad nacional de certificación de la ciberseguridad compartirá la información pertinente recibida en virtud del artículo 37 con otras autoridades nacionales de certificación de la ciberseguridad y ENISA.

2. Otras autoridades nacionales de certificación de la ciberseguridad podrán decidir seguir analizando la vulnerabilidad o, tras informar al titular del certificado EUCC, solicitar a los organismos de certificación pertinentes que determinen si la vulnerabilidad puede afectar a otros productos de TIC certificados.

Artículo 39

Publicación de la vulnerabilidad

Tras la retirada del certificado, el titular del certificado EUCC divulgará y registrará toda vulnerabilidad conocida públicamente y subsanada en el producto de TIC en la base de datos europea de vulnerabilidades, creada de conformidad

con el artículo 12 de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo ([5]) o en otros registros en línea a que se refiere el artículo 55, apartado 1, letra d), del Reglamento (UE) 2019/881.

CAPÍTULO VII

CONSERVACIÓN, DIVULGACIÓN Y PROTECCIÓN DE LA INFORMACIÓN

Artículo 40

Conservación de registros por parte de los organismos de certificación y las ITSEF

1. Las ITSEF y los organismos de certificación mantendrán un sistema de registro, que incluirá todos los documentos presentados en relación con cada evaluación y certificación que realicen.

2. Los organismos de certificación y las ITSEF conservarán los registros de manera segura durante el período necesario para los fines del presente Reglamento y, como mínimo, durante los cinco años siguientes a la retirada del correspondiente certificado EUCC. Cuando el organismo de certificación haya expedido un nuevo certificado EUCC de conformidad con el artículo 13, apartado 2, letra c), conservará la documentación del certificado EUCC retirado junto con el nuevo certificado EUCC y durante el mismo tiempo.

Artículo 41

Información puesta a disposición por el titular de un certificado

1. La información a que se refiere el artículo 55 del Reglamento (UE) 2019/881 estará disponible en un lenguaje fácilmente accesible para los usuarios.

2. Los titulares de certificados EUCC conservarán de forma segura durante el período necesario para los fines del presente Reglamento y, como mínimo, durante los cinco años siguientes a la retirada de los correspondientes certificados EUCC los siguientes elementos:

a) registros de la información facilitada al organismo de certificación y a la ITSEF durante el proceso de certificación,

b) muestra del producto de TIC certificado.

3. Cuando el organismo de certificación haya expedido un nuevo certificado EUCC de conformidad con el artículo 13, apartado 2, letra c), el titular conservará la documentación del certificado EUCC retirado junto con el nuevo certificado EUCC y durante el mismo tiempo.

4. A petición del organismo de certificación o de la autoridad nacional de certificación de la ciberseguridad, los titulares de certificados EUCC pondrán a disposición los registros y las copias a que se refiere el apartado 2.

Artículo 42

Información que debe publicar ENISA

1. ENISA publicará en el sitio web a que se refiere el artículo 50, apartado 1, del Reglamento (UE) 2019/881 la siguiente información:

a) todos los certificados EUCC;

b) información sobre el estado de un certificado EUCC, en particular si está en vigor, si se ha suspendido o retirado, o si ha expirado;

c) los informes de certificación correspondientes a cada certificado EUCC;

([5]) 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).

d) una lista de los organismos de evaluación de la conformidad acreditados;

e) una lista de los organismos de evaluación de la conformidad autorizados;

f) los documentos del estado de la técnica enumerados en el anexo I;

g) los dictámenes del Grupo Europeo de Certificación de la Ciberseguridad a que se refiere el artículo 62, apartado 4, letra c), del Reglamento (UE) 2019/881;

h) los informes de evaluación por pares emitidos de conformidad con el artículo 47.

2. La información a que se refiere el apartado 1 deberá publicarse, como mínimo, en inglés.

3. Los organismos de certificación y, en su caso, las autoridades nacionales de certificación de la ciberseguridad informarán sin demora a ENISA de sus decisiones que afecten al contenido o al estado de un certificado EUCC a que se refiere el apartado 1, letra b).

4. ENISA velará por que la información publicada de conformidad con el apartado 1, letras a), b) y c), determine claramente las versiones de cada producto de TIC certificado que se encuentran cubiertas por el certificado EUCC.

Artículo 43

Protección de la información

Los organismos de evaluación de la conformidad, las autoridades nacionales de certificación de la ciberseguridad, el Grupo Europeo de Certificación de la Ciberseguridad, ENISA, la Comisión y todas las demás partes velarán por la seguridad y protección de los secretos empresariales y otra información confidencial, incluidos los secretos comerciales, así como por la preservación de los derechos de propiedad intelectual e industrial, y adoptarán las medidas técnicas y organizativas necesarias y adecuadas.

CAPÍTULO VIII

ACUERDOS DE RECONOCIMIENTO MUTUO CON TERCEROS PAÍSES

Artículo 44

Condiciones

1. Los terceros países que deseen certificar sus productos con arreglo al presente Reglamento y que dicha certificación se reconozca en la Unión celebrarán un acuerdo de reconocimiento mutuo con esta última.

2. El acuerdo de reconocimiento mutuo abarcará los niveles de garantía aplicables a los productos de TIC certificados y, en su caso, a los perfiles de protección.

3. Los acuerdos de reconocimiento mutuo a que se refiere el apartado 1 solo podrán celebrarse con terceros países que cumplan las siguientes condiciones:

a) disponer de una autoridad que:

   1) sea un organismo público, independiente de las entidades que supervise y controle en materia de estructura organizativa y jurídica, recursos financieros y toma de decisiones;

   2) cuente con las competencias adecuadas de supervisión y control para llevar a cabo investigaciones y esté facultada para adoptar las medidas correctoras oportunas para garantizar el cumplimiento;

   3) posea un régimen sancionador eficaz, proporcionado y disuasorio para garantizar el cumplimiento;

   4) acepte colaborar con el Grupo Europeo de Certificación de la Ciberseguridad y ENISA para intercambiar las mejores prácticas y la evolución pertinente en el ámbito de la certificación de la ciberseguridad y procurar una interpretación uniforme de los criterios y métodos de evaluación actualmente aplicables, entre otras cosas, mediante la utilización de documentación armonizada equivalente a los documentos del estado de la técnica enumerados en el anexo I;

b) contar con un organismo de acreditación independiente que lleve a cabo acreditaciones con arreglo a normas equivalentes a las mencionadas en el Reglamento (CE) n.º 765/2008;

c) comprometerse a que los procesos y procedimientos de evaluación y certificación se lleven a cabo con la debida profesionalidad, teniendo en cuenta el cumplimiento de las normas internacionales a que se refiere el presente Reglamento, en particular en su artículo 3;

d) tener la capacidad de notificar vulnerabilidades no detectadas anteriormente y haber establecido un procedimiento adecuado de gestión y divulgación de vulnerabilidades;

e) haber establecido procedimientos que le permitan presentar y tramitar eficazmente las reclamaciones y ofrecer vías de recurso efectivas a los reclamantes;

f) establecer un mecanismo de cooperación con otros organismos de la Unión y de los Estados miembros competentes en materia de certificación de la ciberseguridad en virtud del presente Reglamento, que comprenda la facilitación de información sobre posibles incumplimientos de los certificados, el seguimiento de la evolución pertinente en el ámbito de la certificación y la adopción de un enfoque conjunto con respecto al mantenimiento y la revisión de las certificaciones.

4. Además de las condiciones establecidas en el apartado 3, para poder celebrar un acuerdo de reconocimiento mutuo a que se refiere el apartado 1 que abarque el nivel de garantía «elevado» con un tercer país, también deberán cumplirse las siguientes condiciones:

a) que el tercer país disponga de una autoridad independiente y pública de certificación de la ciberseguridad que lleve a cabo o delegue las actividades de evaluación necesarias para permitir la certificación con un nivel de garantía «elevado» que sean equivalentes a los requisitos y procedimientos establecidos para las autoridades nacionales de ciberseguridad en el presente Reglamento y en el Reglamento (UE) 2019/881;

b) que el acuerdo de reconocimiento mutuo establezca un mecanismo conjunto equivalente a la evaluación por pares para la certificación EUCC con el fin de mejorar el intercambio de prácticas y resolver conjuntamente los problemas planteados en el ámbito de la evaluación y la certificación.

CAPÍTULO IX

EVALUACIÓN POR PARES DE ORGANISMOS DE CERTIFICACIÓN

Artículo 45

Procedimiento de evaluación por pares

1. Los organismos de certificación que expidan certificados EUCC con un nivel de garantía «elevado» se someterán a una evaluación por pares de forma periódica y, como mínimo, cada cinco años. Los diferentes tipos de evaluación por pares se enumeran en el anexo VI.

2. El Grupo Europeo de Certificación de la Ciberseguridad elaborará y mantendrá un calendario de evaluaciones por pares que garantice el respeto de dicha periodicidad. Salvo en casos debidamente justificados, las evaluaciones por pares se llevarán a cabo *in situ*.

3. La evaluación por pares podrá basarse en pruebas recabadas en el transcurso de anteriores evaluaciones por pares o procedimientos equivalentes del organismo de certificación sometido a dicha evaluación o la autoridad nacional de certificación de la ciberseguridad, siempre que:

a) los resultados no tengan más de cinco años;

b) los resultados vayan acompañados de una descripción de los procedimientos de evaluación por pares establecidos para dicho esquema cuando se refieran a una evaluación por pares realizada con arreglo a otro esquema de certificación;

c) el informe de evaluación por pares a que se refiere el artículo 47 especifique qué resultados se han reutilizado con o sin otra evaluación.

4. Cuando una evaluación por pares abarque un ámbito técnico, también se evaluará la ITSEF interesada.

5. El organismo de certificación sometido a la evaluación por pares y, en caso necesario, la autoridad nacional de certificación de la ciberseguridad velarán por que toda la información pertinente se ponga a disposición del equipo de evaluación por pares.

6. La evaluación por pares será llevada a cabo por un equipo de evaluación por pares constituido de conformidad con el anexo VI.

Artículo 46

Fases de la evaluación por pares

1. Durante la fase preparatoria, los miembros del equipo de evaluación por pares revisarán la documentación del organismo de certificación, que abarcará sus políticas y procedimientos, incluido el uso de documentos del estado de la técnica.

2. Durante la fase de visita de las instalaciones, el equipo de evaluación por pares evaluará la competencia técnica del organismo y, en su caso, la competencia de la ITSEF que haya realizado, como mínimo, una evaluación de productos de TIC cubierta por la evaluación por pares.

3. La duración de la fase de visita de las instalaciones podrá ampliarse o reducirse en función de factores tales como la posibilidad de reutilizar pruebas y resultados de anteriores evaluaciones por pares o el número de ITSEF y de ámbitos técnicos para los que el organismo de certificación expide certificados.

4. Si procede, el equipo de evaluación por pares determinará la competencia técnica de cada ITSEF mediante la visita de su laboratorio o laboratorios técnicos y la entrevista de sus evaluadores en relación con el ámbito técnico y los métodos de ataque específicos conexos.

5. En la fase de información, el equipo de evaluación documentará sus constataciones en un informe de evaluación por pares que contenga un dictamen y, en su caso, una lista de las faltas de conformidad observadas, calificadas individualmente con su correspondiente nivel de criticidad.

6. El informe de evaluación por pares deberá debatirse en primer lugar con el organismo de certificación sometido a dicha evaluación. Tras estos debates, el organismo de certificación sometido a la evaluación por pares establecerá un calendario de las medidas que deben adoptarse para abordar las constataciones.

Artículo 47

Informe de evaluación por pares

1. El equipo de evaluación por pares proporcionará al organismo de certificación sometido a dicha evaluación un proyecto de informe de evaluación por pares.

2. El organismo de certificación sometido a la evaluación por pares presentará al equipo de evaluación por pares sus observaciones acerca de las constataciones y una lista de compromisos para subsanar las deficiencias detectadas en el citado proyecto de informe.

3. El equipo de evaluación por pares presentará al Grupo Europeo de Certificación de la Ciberseguridad un informe final de evaluación por pares, que contendrá asimismo las observaciones y los compromisos formulados por el organismo de certificación sometido a dicha evaluación. El equipo de evaluación por pares también incluirá su postura sobre las observaciones y sobre si los compromisos contraídos son suficientes para subsanar las deficiencias detectadas.

4. En caso de que el informe de evaluación por pares detecte faltas de conformidad, el Grupo Europeo de Certificación de la Ciberseguridad podrá fijar un plazo adecuado para que el organismo de certificación sometido a la evaluación por pares las subsane.

5. El Grupo Europeo de Certificación de la Ciberseguridad adoptará un dictamen sobre el informe de evaluación por pares:

a) cuando el informe de evaluación por pares no detecte faltas de conformidad o cuando el organismo de certificación sometido a dicha evaluación las haya subsanado adecuadamente, el Grupo Europeo de Certificación de la Ciberseguridad podrá emitir un dictamen favorable y todos los documentos pertinentes se publicarán en el sitio web de certificación de ENISA;

b) cuando el organismo de certificación sometido a la evaluación por pares no subsane adecuadamente las faltas de conformidad dentro del plazo fijado, el Grupo Europeo de Certificación de la Ciberseguridad podrá emitir un dictamen negativo que se publicará en el sitio web de certificación de ENISA junto con el informe de evaluación por pares y todos los documentos pertinentes.

6. Antes de la publicación del dictamen, se eliminará de los documentos que vayan a publicarse toda información delicada, personal o de dominio privado.

CAPÍTULO X

MANTENIMIENTO DEL ESQUEMA

Artículo 48

Mantenimiento del EUCC

1. La Comisión podrá solicitar al Grupo Europeo de Certificación de la Ciberseguridad que adopte un dictamen con vistas al mantenimiento del EUCC y que lleve a cabo los trabajos preparatorios necesarios.

2. El Grupo Europeo de Certificación de la Ciberseguridad podrá adoptar un dictamen para aprobar documentos del estado de la técnica.

3. Los documentos del estado de la técnica que hayan sido aprobados por el Grupo Europeo de Certificación de la Ciberseguridad serán publicados por ENISA.

CAPÍTULO XI

DISPOSICIONES FINALES

Artículo 49

Esquemas nacionales cubiertos por el EUCC

1. De conformidad con el artículo 57, apartado 1, del Reglamento (UE) 2019/881 y sin perjuicio de lo dispuesto en el artículo 57, apartado 3, de dicho Reglamento, todos los esquemas nacionales de certificación de la ciberseguridad y los procedimientos correspondientes para los productos y procesos de TIC cubiertos por el EUCC dejarán de surtir efectos transcurridos doce meses desde la entrada en vigor del presente Reglamento.

2. No obstante lo dispuesto en el artículo 50, podrán iniciarse procesos de certificación conforme a un esquema nacional de certificación de la ciberseguridad en un plazo de doce meses a partir de la entrada en vigor del presente Reglamento, siempre que finalicen a más tardar veinticuatro meses después de dicha entrada en vigor.

3. Los certificados expedidos en virtud de esquemas nacionales de certificación de la ciberseguridad podrán ser objeto de revisión. Los nuevos certificados que sustituyan a los certificados revisados se expedirán de conformidad con el presente Reglamento.

Artículo 50

Entrada en vigor

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

Será aplicable a partir del 27 de febrero de 2025.

El capítulo IV y el anexo V se aplicarán a partir de la fecha de entrada en vigor del presente Reglamento.

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

Hecho en Bruselas, el 31 de enero de 2024.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

ANEXO I

Ámbitos técnicos y documentos del estado de la técnica

1. Ámbitos técnicos en los niveles AVA_VAN.4 o AVA_VAN.5:

   a) documentos relacionados con la evaluación armonizada del ámbito técnico «tarjetas inteligentes y dispositivos similares» y, en particular, los siguientes en sus respectivas versiones que estén en vigor el [fecha de entrada en vigor]:

      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», documento en inglés], aprobados inicialmente por el Grupo Europeo de Certificación de la Ciberseguridad el 20 de octubre de 2023;

      2) Minimum Site Security Requirements [«Requisitos mínimos de seguridad de las instalaciones», documento en inglés], aprobados inicialmente por el Grupo Europeo de Certificación de la Ciberseguridad el 20 de octubre de 2023;

      3) Application of Common Criteria to integrated circuits [«Aplicación de los criterios comunes a los circuitos integrados», documento en inglés], aprobada inicialmente por el Grupo Europeo de Certificación de la Ciberseguridad el 20 de octubre de 2023;

      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», documento en inglés], aprobados inicialmente por el Grupo Europeo de Certificación de la Ciberseguridad el 20 de octubre de 2023;

      5) Certification of «open» smart card products [«Certificación de productos de tarjeta inteligente "abierta"», documento en inglés], aprobada inicialmente por el Grupo Europeo de Certificación de la Ciberseguridad el 20 de octubre de 2023;

      6) Composite product evaluation for smart cards and similar devices [«Evaluación de productos compuestos para tarjetas inteligentes y dispositivos similares», documento en inglés], aprobada inicialmente por el Grupo Europeo de Certificación de la Ciberseguridad el 20 de octubre de 2023;

      7) Application of Attack Potential to Smartcards [«Aplicación de potencial de ataque a tarjetas inteligentes», documento en inglés], aprobada inicialmente por el Grupo Europeo de Certificación de la Ciberseguridad el 20 de octubre de 2023;

   b) documentos relacionados con la evaluación armonizada del ámbito técnico «dispositivos de hardware con cajas de seguridad» y, en particular, los siguientes documentos en sus respectivas versiones en vigor el [fecha de entrada en vigor]:

      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», documento en inglés], aprobados inicialmente por el Grupo Europeo de Certificación de la Ciberseguridad el 20 de octubre de 2023;

      2) Minimum Site Security Requirements [«Requisitos mínimos de seguridad de las instalaciones», documento en inglés], aprobados inicialmente por el Grupo Europeo de Certificación de la Ciberseguridad el 20 de octubre de 2023;

      3) Application of Attack Potential to Hardware Devices with Security Boxes [«Aplicación de potencial de ataque a dispositivos de hardware con cajas de seguridad», documento en inglés], aprobada inicialmente por el Grupo Europeo de Certificación de la Ciberseguridad el 20 de octubre de 2023.

2. Documentos del estado de la técnica en sus respectivas versiones en vigor a [fecha de entrada en vigor]:

   a) documento relativo a la acreditación armonizada de los organismos de evaluación de la conformidad: *Accreditation of ITSEFs for the EUCC* [«Acreditación de ITSEF a efectos del EUCC», documento en inglés], aprobada inicialmente por el Grupo Europeo de Certificación de la Ciberseguridad el 20 de octubre de 2023.

ANEXO II

Perfiles de protección certificados en los niveles AVA_VAN.4 o AVA_VAN.5

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

1) UNE-EN 419241-2: 2019 «Sistemas confiables que permiten firma de servidor. Parte 2: Perfil de protección de QSCD para la firma del servidor»;

2) 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»

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

[EN BLANCO]

ANEXO III

Perfiles de protección recomendados (ilustran los ámbitos técnicos del anexo I)

Perfiles de protección utilizados en la certificación de productos de TIC pertenecientes a las categorías de productos de TIC enumeradas a continuación:

a) para la categoría de documentos de viaje de lectura mecánica [disponibles en inglés]:

1) «PP for a Machine Readable Travel Document using Standard Inspection Procedure with PACE» [«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)»], BSI-CC-PP-0068-V2-2011-MA-01;

2) «PP for a Machine Readable Travel Document with "ICAO Application" Extended Access Control» [«PP para documentos de viaje de lectura mecánica con control de acceso ampliado basado en la aplicación de las normas de la Organización de Aviación Civil Internacional (OACI)»], BSI-CC-PP-0056-2009;

3) «PP for a 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»], BSI-CC-PP-0056-V2-2012-MA-02;

4) «PP for a 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»], BSI-CC-PP-0055-2009;

b) para la categoría de dispositivos seguros de creación de firma:

1) UNE-EN 419211-1:2014 «Perfiles de protección para los dispositivos seguros de creación de firma. Parte 1: Visión general»

2) UNE-EN 419211-2:2013 «Perfiles de protección para los dispositivos seguros de creación de firma. Parte 2: Dispositivo con generación de claves»;

3) UNE-EN 419211-3:2013 «Perfiles de protección para los dispositivos seguros de creación de firma. Parte 3: Dispositivo con importación de claves»;

4) 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 canal seguro con la aplicación de generación de certificado»;

5) 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 canal seguro con la aplicación de creación de firma»;

6) 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 canal seguro con la aplicación de creación de firma»;

c) para la categoría de tacógrafos digitales:

1) tacógrafo digital: tarjeta de tacógrafo, tal como consta en el 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 (anexo 1 C);

2) tacógrafo digital: unidad intravehicular, tal como consta en el anexo I B del Reglamento (CE) n.º 1360/2002 de la Comisión, a saber, concebida para ser instalada en vehículos de transporte por carretera;

3) tacógrafo digital: dispositivo GNSS externo («PP EGF», por sus siglas en inglés), tal como consta en el anexo 1 C del 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;

4) tacógrafo digital: sensor de movimiento («PP MoS», por sus siglas en inglés), tal como consta en el anexo 1 C del 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;

d) para la categoría de circuitos integrados seguros, tarjetas inteligentes y dispositivos conexos [disponibles en inglés]:

1) «Security IC Platform PP» [«PP para plataformas de circuitos integrados de seguridad»], BSI-CC-PP-0084-2014;

2) «Java Card System – Open Configuration» [«Sistema Java Card: configuración abierta»], V3.0.5 BSI-CC-PP-0099-2017;

3) «Java Card System – Closed Configuration» [«Sistema Java Card: configuración cerrada»], BSI-CC-PP-0101-2017;

4) «PP for a PC Client Specific Trusted Platform Module Family 2.0 Level 0 Revision 1.16» [«PP para módulo de plataforma segura específico de PC clientes, familia 2.0, nivel 0, revisión 1.16»], ANSSI-CC-PP-2015/07;

5) «Universal SIM Java Card Platform» [«Plataforma de módulo de identificación de usuario (SIM) universal Java Card»], PU-2009-RT-79, ANSSI-CC-PP-2010/04;

6) «Embedded UICC (eUICC) for Machine-to-Machine Devices» [«Tarjeta universal de circuito integrado incorporada (eUICC) para dispositivos de máquina a máquina»], BSI-CC-PP-0089-2015;

e) para la categoría de puntos de interacción (de pago) y terminales de pago [disponibles en inglés]:

1) Punto de interacción «POI-CHIP-ONLY», ANSSI-CC-PP-2015/01;

2) Punto de interacción «POI-CHIP-ONLY and Open Protocol Package» [«POI-CHIP-ONLY y paquete de protocolos abiertos»], ANSSI-CC-PP-2015/02;

3) Punto de interacción «POI-COMPREHENSIVE», ANSSI-CC-PP-2015/03;

4) Punto de interacción «POI-COMPREHENSIVE and Open Protocol Package», ANSSI-CC-PP-2015/04;

5) Punto de interacción «POI-PED-ONLY», ANSSI-CC-PP-2015/05;

6) Punto de interacción «POI-PED-ONLY and Open Protocol Package», ANSSI-CC-PP-2015/06;

f) para la categoría de dispositivos de *hardware* con cajas de seguridad [disponibles en inglés]:

1) «Cryptographic Module for CSP Signing Operations with Backup – PP CMCSOB» [«Módulo criptográfico para operaciones de firma de proveedores de servicios de certificación (PSC) con copia de seguridad (“PP CMCSOB”, por sus siglas en inglés)»], PP HSM CMCSOB 14167-2, ANSSI-CC-PP-2015/08;

2) «Cryptographic Module for CSP key generation services – PP CMCKG» [«Módulo criptográfico para servicios de generación de claves de PSC (“PP CMCKG”, por sus siglas en inglés)»], PP HSM CMCKG 14167-3, ANSSI-CC-PP-2015/09;

3) Cryptographic Module for CSP Signing Operations without Backup – PP CMCSO [«Módulo criptográfico para operaciones de firma de PSC sin copia de seguridad» (“PP CMCSO”, por sus siglas en inglés)], PP HSM CMCKG 14167-4, ANSSI-CC-PP-2015/10.

ANEXO IV

Continuidad de la garantía y revisión de los certificados

IV.1 Continuidad de la garantía: ámbito de aplicación

1. Se aplicarán los siguientes requisitos para la continuidad de la garantía a las actividades de mantenimiento relacionadas con los siguientes aspectos:

   a) una revaluación para determinar si un producto de TIC certificado que no haya sufrido modificaciones sigue cumpliendo sus requisitos de seguridad;

   b) una evaluación de los efectos de las modificaciones de un producto de TIC certificado en su certificación;

   c) si se incluye en la certificación, la aplicación de parches de seguridad con arreglo a un proceso de gestión de parches evaluado;

   d) si se incluye, la revisión de los procesos de gestión del ciclo de vida o de producción del titular del certificado.

2. El titular de un certificado EUCC podrá solicitar la revisión del certificado en los siguientes casos:

   a) cuando el certificado EUCC vaya a expirar en un plazo de nueve meses;

   b) cuando se haya producido un cambio en el producto de TIC certificado o en otro factor que pueda afectar a su funcionalidad de seguridad;

   c) cuando el titular del certificado solicite que se repita la evaluación de vulnerabilidad con el fin de volver a confirmar la garantía del certificado EUCC asociada a la resistencia del producto de TIC frente a los ciberataques actuales.

IV.2 Revaluación

1. Cuando sea necesario determinar los efectos de los cambios producidos en el entorno de amenazas de un producto de TIC certificado que no haya sufrido modificaciones, se presentará una solicitud de revaluación al organismo de certificación.

2. La revaluación será llevada a cabo por la misma ITSEF que participó en la evaluación anterior y se reutilizarán todos los resultados que sigan vigentes. La evaluación se centrará en las actividades de garantía que puedan verse afectadas por los cambios del entorno de amenazas del producto de TIC certificado, en particular la familia AVA_VAN pertinente y, además, la familia del ciclo de vida de la garantía («ALC», por sus siglas en inglés), en las que se volverán a recabar pruebas suficientes del mantenimiento del entorno de desarrollo.

3. La ITSEF describirá los cambios producidos y detallará los resultados de la revaluación con una actualización del informe técnico de evaluación anterior.

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.

5. El informe de revaluación y el certificado actualizado se transmitirán a la autoridad nacional de certificación de la ciberseguridad y a ENISA para su publicación en su sitio web de certificación de la ciberseguridad.

IV.3 Modificaciones de un producto de TIC certificado

1. Cuando un producto de TIC certificado haya sufrido modificaciones, el titular que desee mantener el certificado facilitará al organismo de certificación un informe de evaluación de impacto.

2. El informe de evaluación de impacto contendrá los siguientes elementos:

   a) una introducción con la información necesaria para identificar el informe de evaluación de impacto y el objeto de evaluación modificado;

b) una descripción de las modificaciones introducidas en el producto;

c) la identificación de las pruebas aportadas por el desarrollador afectado;

d) una descripción de las modificaciones de las pruebas aportadas por el desarrollador;

e) las constataciones y conclusiones sobre los efectos de cada modificación en la garantía.

3. El organismo de certificación examinará las modificaciones descritas en el informe de evaluación de impacto para validar sus efectos en la garantía del objeto de evaluación certificado, tal como se proponga en las conclusiones del informe de evaluación de impacto.

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

5. Cuando el organismo de certificación haya confirmado que las modificaciones son menores, se expedirá un nuevo certificado para el producto de TIC modificado y se elaborará un informe de mantenimiento del informe de certificación inicial, con las siguientes condiciones:

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

1) introducción;

2) descripción de las modificaciones;

3) pruebas aportadas por el desarrollador afectado;

b) la fecha de validez del nuevo certificado no sobrepasará la fecha del certificado inicial.

6. El nuevo certificado se transmitirá a ENISA con su correspondiente informe de mantenimiento para que lo publique en su sitio web de certificación de la ciberseguridad.

7. En caso de que se confirme que las modificaciones son importantes, se llevará a cabo una revaluación en el contexto de la evaluación anterior y se reutilizarán todos los resultados de esta última que sigan vigentes.

8. Una vez finalizada la evaluación del objeto de evaluación modificado, la ITSEF elaborará un nuevo informe técnico de evaluación. El organismo de certificación revisará el informe técnico de evaluación actualizado y, cuando proceda, elaborará un nuevo certificado con un nuevo informe de certificación.

9. El nuevo certificado y el nuevo informe de certificación se transmitirán a ENISA para su publicación.

IV.4 **Gestión de parches**

1. El procedimiento de gestión de parches prevé un proceso estructurado de actualización de un producto de TIC certificado. Dicho procedimiento, que incluye el mecanismo aplicado al producto de TIC por el solicitante de la certificación, puede utilizarse tras la certificación del producto de TIC bajo la responsabilidad del organismo de evaluación de la conformidad.

2. El solicitante de la certificación podrá incluir en la certificación del producto de TIC un mecanismo de parches como parte de un procedimiento de gestión certificado aplicado al producto de TIC cuando se cumpla una de las siguientes condiciones:

a) que las funcionalidades afectadas por el parche queden fuera del objeto de evaluación del producto de TIC certificado;

b) que el parche se refiera a una modificación menor predeterminada en el producto de TIC certificado;

c) que el parche se refiera a una vulnerabilidad confirmada con efectos críticos en la seguridad del producto de TIC certificado.

3. Si el parche está relacionado con una modificación importante del objeto de evaluación del producto de TIC certificado con respecto a una vulnerabilidad no detectada anteriormente que no tenga efectos críticos en la seguridad del producto de TIC, se aplicará lo dispuesto en el artículo 13.

4. El procedimiento de gestión de parches de un producto de TIC constará de los siguientes elementos:

   a) el proceso de desarrollo y lanzamiento del parche para el producto de TIC;

   b) el mecanismo técnico y las funciones para la aplicación del parche en el producto de TIC;

   c) un conjunto de actividades de evaluación relacionadas con la eficacia y el rendimiento del mecanismo técnico.

5. En el proceso de certificación del producto de TIC:

   a) el solicitante de la certificación del producto de TIC proporcionará la descripción del procedimiento de gestión de parches;

   b) la ITSEF realizará las siguientes comprobaciones:

      1) que el desarrollador haya implementado los mecanismos de parches en el producto de TIC con arreglo al procedimiento de gestión de parches presentado para su certificación;

      2) que el perímetro del objeto de evaluación se haya delimitado de manera que los cambios introducidos en los procesos separados no afecten a la seguridad del objeto de evaluación;

      3) que el mecanismo técnico de parches funcione de conformidad con lo dispuesto en la presente sección y con lo declarado por el solicitante;

   c) el organismo de certificación incluirá en el informe de certificación el resultado de la evaluación del procedimiento de gestión de parches.

6. El titular del certificado podrá proceder a aplicar el parche elaborado de conformidad con el procedimiento de gestión de parches certificado al producto de TIC certificado de que se trate y adoptará las siguientes medidas en un plazo de cinco días laborables en los casos que se indican a continuación:

   a) en el caso a que se refiere el punto 2, letra a), informará del parche de que se trate al organismo de certificación, que no modificará el certificado EUCC correspondiente;

   b) en el caso a que se refiere el punto 2, letra b), presentará el parche de que se trate a la ITSEF para su revisión, y esta informará al organismo de certificación tras la recepción del parche para que adopte las medidas adecuadas con respecto a la expedición de una nueva versión del certificado EUCC correspondiente y la actualización del informe de certificación;

   c) en el caso a que se refiere el punto 2, letra c), presentará el parche de que se trate a la ITSEF para su necesaria revaluación, pero podrá desplegarlo paralelamente; por su parte, la ITSEF informará al organismo de certificación, que procederá entonces a iniciar las actividades de certificación correspondientes.

ANEXO V

Contenido de los informes de certificación

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.

2. El informe de certificación es la fuente de información detallada y práctica sobre el producto de TIC o la categoría de productos 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 constará, como mínimo, de las siguientes secciones:

   a) resumen;

   b) identificación del producto de TIC o de la categoría de productos de TIC en el caso de los perfiles de protección;

   c) servicios de seguridad;

   d) hipótesis y aclaración del ámbito de aplicación;

   e) información arquitectónica;

   f) información complementaria sobre ciberseguridad, en su caso;

   g) ensayo del producto de TIC, en caso de haberse realizado;

   h) cuando proceda, identificación de los procesos de gestión del ciclo de vida y las instalaciones de producción del titular del certificado;

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

   j) resumen de la declaración de seguridad del producto de TIC presentado para su certificación;

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

   l) bibliografía.

4. El resumen 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, enumeración de los componentes del producto que forman parte de la evaluación y versión del producto de TIC;

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

   c) fecha de conclusión de la evaluación;

   d) referencia al informe técnico de evaluación elaborado por la ITSEF;

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

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

      2) los componentes de garantía de seguridad y el paquete de garantía de los criterios comunes, en particular 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;

      3) la funcionalidad de seguridad del producto de TIC evaluado;

      4) un resumen de las amenazas y las políticas de seguridad organizativas abordadas por el producto de TIC evaluado;

5) requisitos especiales de configuración;

6) hipótesis sobre el entorno operativo;

7) en su caso, la presencia de un procedimiento de gestión de parches aprobado de conformidad con la sección IV.4 del anexo IV;

8) cláusula(s) de exención de responsabilidad.

5. El producto de TIC evaluado se identificará claramente, especificando en particular la siguiente información:

a) denominación del producto de TIC evaluado;

b) enumeración de los componentes del producto de TIC que forman parte de la evaluación;

c) número de versión de los componentes del producto de TIC;

d) determinación de requisitos adicionales para el entorno operativo del producto de TIC certificado;

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

f) en su caso, procedimiento de gestión de parches incluido en el certificado;

g) enlace al sitio web del titular del certificado EUCC en el que se facilita información complementaria sobre ciberseguridad con respecto al producto de TIC certificado, de conformidad con el artículo 55 del Reglamento (UE) 2019/881.

6. La información incluida en la presente sección será lo más precisa posible para garantizar una representación completa y precisa del producto de TIC que pueda reutilizarse en futuras evaluaciones.

7. La sección relativa a la política de seguridad contendrá la descripción de la política de seguridad del producto de TIC y de las políticas o normas que el producto de TIC evaluado deba aplicar o cumplir. Incluirá una referencia y una descripción de las siguientes políticas:

a) política de gestión de vulnerabilidades del titular del certificado;

b) política de continuidad de la garantía del titular del certificado.

8. Cuando proceda, la política podrá especificar las condiciones relativas al uso de un procedimiento de gestión de parches durante el período de validez del certificado.

9. La sección relativa a las hipótesis y la aclaración del ámbito de aplicación contendrá información exhaustiva 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.

10. La información enumerada en el punto 9 será lo más comprensible posible para que los usuarios del producto de TIC certificado puedan tomar decisiones con conocimiento de causa sobre los riesgos asociados a su uso.

11. La sección de información arquitectónica contendrá una descripción de alto nivel del producto de TIC y sus principales componentes con arreglo al diseño de subsistemas ADV_TDS de los criterios comunes.

12. Se proporcionará una lista completa de la información complementaria sobre ciberseguridad del producto de TIC de conformidad con el artículo 55 del Reglamento (UE) 2019/881. Toda la documentación pertinente se indicará mediante los números de versión.

13. La sección de ensayo del producto de TIC incluirá la siguiente información:

a) nombre y punto de contacto de la autoridad u organismo que haya expedido el certificado, incluida la autoridad nacional de certificación de la ciberseguridad competente;

b) nombre de la ITSEF que haya llevado a cabo la evaluación, cuando difiera del organismo de certificación;

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

d) versión del documento del estado de la técnica y demás criterios de evaluación de la seguridad utilizados en la evaluación;

e) configuración y ajustes completos y precisos del producto de TIC durante la evaluación, incluidas las notas operativas y las observaciones, en su caso;

f) todo perfil de protección que se haya utilizado, especificando la siguiente información:

1) autor del perfil de protección;

2) denominación e identificador del perfil de protección;

3) identificador del certificado del perfil de protección;

4) nombre y datos de contacto del organismo de certificación y de la ITSEF que haya participado en la evaluación del perfil de protección;

5) paquete o paquetes de garantía necesarios para que un producto se ajuste al perfil de protección.

14. La sección de resultados de la evaluación e información relativa al certificado contendrá la siguiente información:

a) confirmación del nivel de garantía alcanzado a que se refieren el artículo 4 del presente Reglamento y el artículo 52 del Reglamento (UE) 2019/881;

b) requisitos de garantía de las normas a que se refiere el artículo 3 que el producto de TIC o el perfil de protección cumpla realmente, incluido el nivel AVA_VAN;

c) descripción detallada de los requisitos de garantía, así como de la manera en que el producto cumple cada uno de ellos;

d) fecha de expedición y período de validez del certificado;

e) identificador único del certificado.

15. La declaración de seguridad se incluirá en el informe de certificación o se citará y resumirá en dicho informe y se adjuntará a este en relación con él a efectos de su publicación.

16. La declaración de seguridad podrá editarse con arreglo a lo dispuesto en la sección VI.2.

17. La marca o etiqueta asociada al EUCC podrá insertarse en el informe de certificación de conformidad con las normas y los procedimientos establecidos en el artículo 11.

18. La sección de bibliografía 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 y su versión;

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) la documentación del desarrollador utilizada en el ejercicio de evaluación.

19. 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.

V.2 **Edición de las declaraciones de seguridad para su publicación**

1. Las declaraciones de seguridad que deban incluirse o citarse en el informe de certificación en virtud de la sección VI.1, punto 1, podrán editarse mediante la supresión o reformulación de información técnica de dominio privado.

2. Las declaraciones de seguridad editadas resultantes constituirán una representación real de su versión original completa. Esto significa que las declaraciones de seguridad editadas no pueden omitir la información necesaria para conocer las propiedades de seguridad del objeto de evaluación y el ámbito de aplicación de la evaluación.

3. El contenido de las declaraciones de seguridad editadas se atendrá a los siguientes requisitos mínimos:
   a) la introducción no se editará, ya que en general no incluye información de dominio privado;
   b) las declaraciones de seguridad editadas deben tener un identificador único distinto del correspondiente a la versión original completa;
   c) la descripción del objeto de evaluación podrá resumirse, ya que es posible que incluya información detallada y de dominio privado sobre el diseño del objeto de evaluación que no debe publicarse;
   d) la descripción del entorno de seguridad del objeto de evaluación (hipótesis, amenazas, políticas de seguridad organizativas) no se resumirá, en la medida en que dicha información sea necesaria para conocer el ámbito de aplicación de la evaluación;
   e) los objetivos de seguridad no se resumirán, ya que toda esta información debe publicarse para dar a conocer la intención de la declaración de seguridad y del objeto de evaluación;
   f) se publicarán todos los requisitos de seguridad: las notas de aplicación pueden proporcionar información sobre la manera en que se han utilizado los requisitos funcionales de los criterios comunes a que se refiere el artículo 3 para entender la declaración de seguridad;
   g) el resumen de las especificaciones del objeto de evaluación incluirá todas sus funciones de seguridad, pero podrá editarse la información adicional de dominio privado;
   h) se incluirán referencias a los perfiles de protección aplicados al objeto de evaluación;
   i) la justificación podrá editarse para suprimir la información de dominio privado.

4. Aunque la declaración de seguridad editada no se evalúa formalmente con arreglo a las normas de evaluación a que se refiere el artículo 3, el organismo de certificación se cerciorará de que se atenga a la declaración de seguridad completa y evaluada, y se remitirá tanto a la declaración de seguridad completa como a la editada en el informe de certificación.

ANEXO VI

Ámbito de aplicación de las evaluaciones por pares y composición del equipo de evaluación

VI.1 Ámbito de aplicación de las evaluaciones por pares

1. Se contemplan los siguientes tipos de evaluaciones por pares:

   a) Tipo 1: cuando un organismo de certificación lleve a cabo actividades de certificación con nivel AVA_VAN.3;

   b) Tipo 2: cuando un organismo de certificación lleve a cabo actividades de certificación relacionadas con un ámbito técnico que figure como documento del estado de la técnica en el anexo I;

   c) Tipo 3: cuando un organismo de certificación lleve a cabo actividades de certificación con un nivel superior a AVA_VAN.3 a partir de un perfil de protección que figure como documento del estado de la técnica en los anexos II o III.

2. El organismo de certificación sometido a una evaluación por pares presentará la lista de productos de TIC certificados que puedan ser candidatos a la revisión por parte del equipo de evaluación por pares, con arreglo a las siguientes normas:

   a) los productos candidatos abarcarán el ámbito técnico de la autorización del organismo de certificación, del que se someterán a la evaluación por pares, como mínimo, las evaluaciones de dos productos diferentes con un nivel de garantía «elevado», y un perfil de protección si el organismo de certificación ha expedido un certificado con nivel de garantía «elevado»;

   b) para las evaluaciones por pares de tipo 2, el organismo de certificación presentará, como mínimo, un producto por ámbito técnico y por ITSEF interesada;

   c) para las evaluaciones por pares de tipo 3, se evaluará, como mínimo, un producto candidato de conformidad con los perfiles de protección aplicables y pertinentes.

VI.2 Equipo de evaluación por pares

1. El equipo de evaluación constará, como mínimo, de dos expertos seleccionados de dos organismos de certificación diferentes de distintos Estados miembros que expidan certificados con nivel de garantía «elevado». Los expertos deben demostrar que poseen los conocimientos especializados pertinentes en relación con las normas a que se refiere el artículo 3 y con los documentos del estado de la técnica comprendidos en el ámbito de aplicación de la evaluación por pares.

2. En los casos de delegación de la expedición de certificados o de aprobación previa de estos a que se refiere el artículo 56, apartado 6, del Reglamento (UE) 2019/881, también podrá participar en el equipo de expertos seleccionado de conformidad con el apartado 1 de la presente sección un experto de la autoridad nacional de certificación de la ciberseguridad relacionada con el organismo de certificación interesado.

3. Para las evaluaciones por pares de tipo 2, los miembros del equipo se seleccionarán a partir de los organismos de certificación autorizados en el ámbito técnico de que se trate.

4. Cada miembro del equipo de evaluación deberá tener, como mínimo, dos años de experiencia en la realización de actividades de certificación en un organismo de certificación.

5. En el caso de las evaluaciones por pares de tipo 2 o 3, cada miembro del equipo de evaluación deberá tener, como mínimo, dos años de experiencia en la realización de actividades de certificación en el ámbito técnico o perfil de protección pertinentes y demostrar que dispone de conocimientos especializados y que ha participado en la autorización de una ITSEF.

6. Participarán en la evaluación por pares en calidad de observadoras la autoridad nacional de certificación de la ciberseguridad que controle y supervise al organismo de certificación sometido a la evaluación por pares y, al menos, una autoridad nacional de certificación de la ciberseguridad cuyo organismo de certificación no esté sujeto a la citada evaluación. ENISA también podrá participar en la evaluación por pares en calidad de observadora.

7. La composición del equipo de evaluación por pares se presenta al organismo de certificación evaluado, que, en casos justificados, podrá impugnar la composición de dicho equipo y solicitar su revisión.

ANEXO VII

Contenido de los certificados EUCC

El certificado EUCC contendrá, como mínimo:

a) un identificador único establecido por el organismo de certificación que expida el certificado;

b) información relacionada con el producto de TIC o el perfil de protección certificados y con el titular del certificado, en particular:

   1) denominación del producto de TIC o del perfil de protección y, en su caso, del objeto de evaluación;

   2) tipo de producto de TIC o de perfil de protección y, en su caso, del objeto de evaluación;

   3) versión del producto de TIC o del perfil de protección;

   4) nombre, dirección e información de contacto del titular del certificado;

   5) enlace al sitio web del titular del certificado que contenga la información complementaria sobre ciberseguridad a que se refiere el artículo 55 del Reglamento (UE) 2019/881;

c) información relacionada con la evaluación y certificación del producto de TIC o el perfil de protección, en particular:

   1) nombre, dirección e información de contacto del organismo de certificación que haya expedido el certificado;

   2) si difiere del organismo de certificación, nombre de la ITSEF que haya llevado a cabo la evaluación;

   3) nombre de la autoridad nacional de certificación de la ciberseguridad competente;

   4) una referencia al presente Reglamento;

   5) una referencia al informe de certificación asociado al certificado a que se refiere el anexo V;

   6) el nivel de garantía aplicable de conformidad con el artículo 4;

   7) una referencia a la versión de las normas utilizadas para la evaluación a que se refiere el artículo 3;

   8) identificación del nivel o paquete de garantía especificado en las normas a que se refiere el artículo 3 y con arreglo a lo dispuesto en el anexo VIII, incluidos los componentes de garantía utilizados y el nivel AVA_VAN cubierto;

   9) en su caso, una referencia al perfil o perfiles de protección que cumpla el producto de TIC o el perfil de protección;

   10) la fecha de expedición;

   11) el período de validez del certificado;

d) la marca y la etiqueta asociadas al certificado de conformidad con el artículo 11.

ANEXO VIII

Declaración del paquete de garantía

1. Contrariamente a las definiciones que figuran en los criterios comunes, las ampliaciones:

a) no se indicarán con la abreviatura «+»;

b) se detallarán mediante una lista de todos los componentes afectados;

c) se describirán minuciosamente en el informe de certificación.

2. El nivel de garantía confirmado en un certificado EUCC podrá complementarse con el nivel de garantía de la evaluación especificado en el artículo 3 del presente Reglamento.

3. Si el nivel de garantía confirmado en un certificado EUCC no se refiere a una ampliación, se indicará en el certificado uno de los siguientes paquetes:

a) «paquete de garantía específico»;

b) «paquete de garantía conforme a un perfil de protección» en caso de remitir a un perfil de protección sin un nivel de garantía de evaluación.

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 del modelo facilitado.

3. En caso de presencia física, la marca y la etiqueta tendrán una altura mínima de 5 mm.