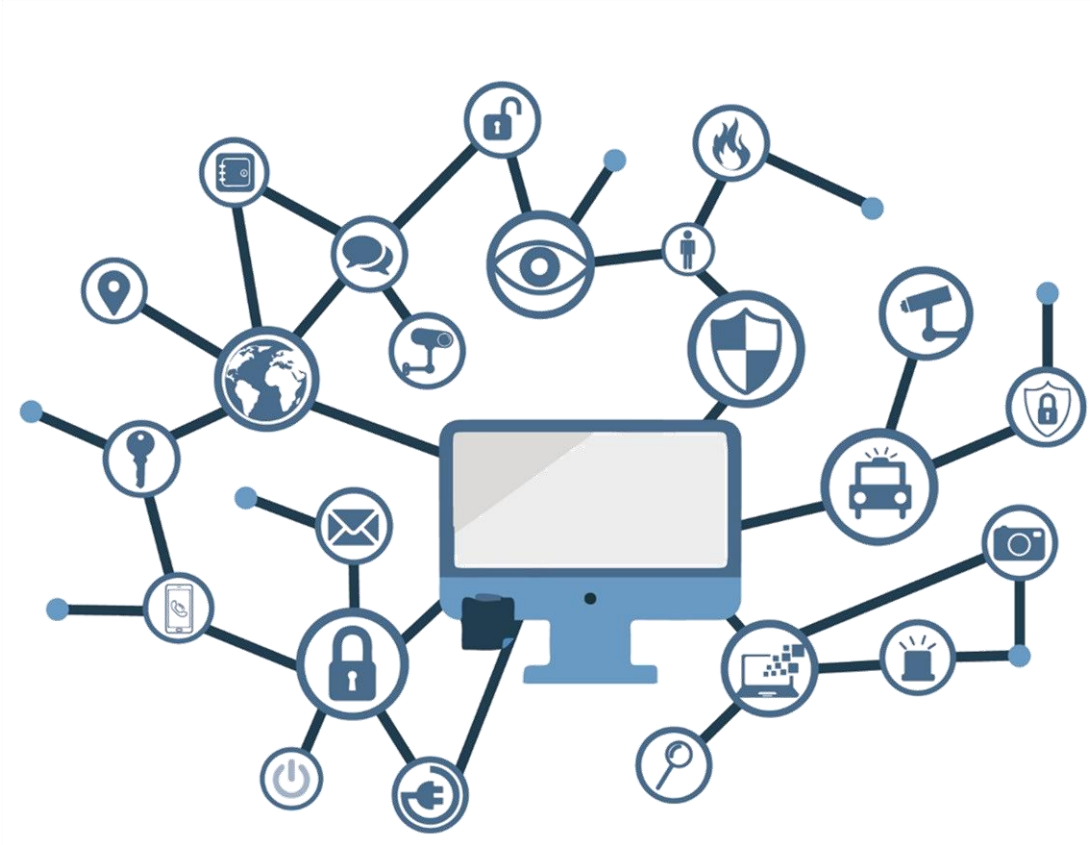
Autoridad Nacional de Certificación de la Ciberseguridad

centro criptológico nacional

ANCC-PO-13

Gestión de vulnerabilidades



Marzo de 2026
Versión 1

MINISTERIO DE DEFENSA

CONTROL DE VERSIONES

Versión	Comentarios
1.0	Versión inicial

ÍNDICE

1. INTRODUCCIÓN

1. El presente documento define los procedimientos y procesos en los que la Autoridad Nacional de Certificación (**ANCC**) desempeña un papel en la gestión de vulnerabilidades de productos, servicios y procesos **TIC** certificados, conforme al **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 (en adelante, **CSA**, por sus siglas en inglés) [CSA], **al 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 en lo concerniente a la adopción del esquema europeo de certificación de ciberseguridad basado en los Criterios Comunes [EUCC]**, y de acuerdo con las **directrices sobre gestión y divulgación de vulnerabilidades [VULMD].**

2. PASOS PREPARATORIOS

2. El jefe de la unidad de la **ANCC (JAN)** publicará, en el sitio web oficial de dicha autoridad **(WANCC),** la información y las orientaciones sobre cómo informar con respecto a las vulnerabilidades por correo electrónico, incluyendo el procedimiento detallado para su tramitación.

3. Se pondrán a disposición formularios (o plantillas) con instrucciones para su cumplimentación. El formulario especificará la información obligatoria que deberá cumplimentarse.

3. PROCEDIMIENTOS DE GESTIÓN DE VULNERABILIDADES

4. La **ANCC** no gestiona directamente las vulnerabilidades, pero ejercerá funciones de supervisión, seguimiento y coordinación, garantizando que las vulnerabilidades que puedan afectar a productos certificados sean tratadas de forma adecuada por los actores responsables, en particular el **titular del certificado** y el *Organismo de Certificación* (**CB**)

3.1 RECEPCIÓN DE INFORMES DE VULNERABILIDAD

5. En el esquema **EUCC**, la gestión inicial de vulnerabilidades corresponde al **titular del certificado**, quien deberá registrar la información recibida y realizar un análisis de impacto de la vulnerabilidad conforme a los requisitos del esquema.

6. La **ANCC** no actúa como punto principal de recepción de vulnerabilidades, no obstante, deberá ser informada en determinados aspectos del proceso de gestión de vulnerabilidades que afecten a productos certificados, en el ejercicio de sus funciones de supervisión.

7. La **ANCC** podrá ser informada de vulnerabilidades, en particular, en los siguientes casos:

    - Cuando el **CB** informe a la **ANCC** de un caso que pueda afectar al estado del certificado, derivado de la validación o evaluación del análisis de impacto de la vulnerabilidad realizado por el titular del certificado
    - Cuando se solicite a la **ANCC** una extensión de plazo en el tratamiento de una vulnerabilidad;

8. Toda comunicación relativa a vulnerabilidades de productos, servicios o procesos TIC certificados podrá dirigirse a **ANCC** a través del correo electrónico cifrado con la clave **PGP** disponible en el sitio web oficial de la autoridad (**WANCC**).

3.2 REGISTRO Y SEGUIMIENTO

9. Para cada formulario o informe de vulnerabilidad recibido se creará o actualizará un registro en el Sistema de Información de la Autoridad Nacional de Certificación de la Ciberseguridad **(SGA)**. El personal técnico de la **ANCC (TA)** designado, registrará todos los detalles pertinentes, incluida la fecha de recepción, titular del certificado, el origen del informe, **CB** responsable de la certificación, la identificación del producto o servicio certificado afectado (con referencia al certificado) y una descripción de la vulnerabilidad.

10. Este registro exhaustivo respalda la transparencia, la trazabilidad y las revisiones posteriores, incluidas las evaluaciones interpares a que se refiere el artículo 45 del **[EUCC]**.

3.3 DECISIÓN SOBRE EXTENSIONES DE PLAZO Y COORDINACIÓN A NIVEL EUROPEO

11. **El titular del certificado EUCC** será el encargado de realizar un análisis de impacto de la vulnerabilidad conforme a los plazos establecidos en el esquema **EUCC** y en la tabla de referencia correspondiente **[VULMD].**

12. En determinados casos, **el titular del certificado** podrá solicitar una **extensión** del plazo establecido para la realización del análisis de impacto o la implementación de medidas correctivas relacionadas con una vulnerabilidad.

13. De conformidad con lo establecido en el esquema **EUCC** y en **[VULMD]**, existen determinadas situaciones en las que el titular del certificado podrá presentar una solicitud de extensión del plazo para la realización del análisis de impacto de la vulnerabilidad.

14. Cuando el titular del certificado considere necesario ampliar el plazo para completar el análisis de impacto de la vulnerabilidad, deberá presentar una solicitud de extensión a la **ANCC**. Esta solicitud deberá remitirse a través del canal de comunicación establecido en la sección *3.1* y será recibida por el jefe de la Unidad de la **ANCC (JAN)**. Tras la recepción de la solicitud, la **ANCC** emitirá un **acuse de recibo de la notificación**.

15. La solicitud deberá realizarse al menos 30 días antes de la finalización del plazo aplicable e incluir:

    - La versión actual del informe de análisis de impacto de la vulnerabilidad, aunque este no esté finalizado;
    - La justificación técnica de la extensión solicitada.

16. El **JAN** asignará un **TA** para el registro en un expediente existente en el **SGA** y para la evaluación técnica de la solicitud de extensión. Dicha evaluación se realizará teniendo en cuenta el posible impacto sobre los usuarios o sobre la sociedad y el impacto en la confianza en el proceso de certificación. La decisión sobre dicha extensión será revisada y aprobada por el **JAN**.

17. Si el titular del certificado no recibe una respuesta a la solicitud de extensión en un plazo de 30 días desde la confirmación de recepción, la solicitud se considerará aceptada por la **ANCC**.

18. El **JAN** deberá informar oportunamente el Grupo Europeo de Certificación de la Ciberseguridad **(GECC)** sobre las extensiones concedidas, con el objetivo de favorecer la armonización del proceso de gestión de vulnerabilidades entre los Estados miembros.

19. En los casos en que el plazo para la elaboración del análisis de impacto de la vulnerabilidad se establezca mediante acuerdo mutuo entre el **CB** y el titular del certificado **EUCC**, la **ANCC** deberá ser informada. Dicha información será registrada por el personal técnico asignado (**TA**) en el **SGA**. El plazo máximo recomendado para este tipo de acuerdos mutuos no debería superar los 180 días.

3.4 SUPERVISIÓN DE DECISIONES

20. La **ANCC** ejercerá funciones de supervisión sobre las decisiones adoptadas por los **CB** en aquellos casos en los que, tras la recepción del informe de análisis de impacto de una vulnerabilidad, el **CB** deba realizar las validaciones correspondientes con el fin de determinar si dicha vulnerabilidad puede afectar a la conformidad del producto con su certificado.

21. Como resultado de esta evaluación, el **CB** podrá adoptar las decisiones que correspondan en relación con el estado del certificado.

22. La **ANCC** deberá ser informada por el **CB**, a través del canal propuesto en la sección 3.1, sobre las validaciones realizadas y las decisiones adoptadas cuando estas puedan tener impacto en el estado del certificado o en la confianza en el esquema de certificación.

23. La información recibida será gestionada por el **JAN** y registrada en el **SGA** por el **TA** designado, con el fin de permitir el seguimiento del caso en el marco de las actividades de supervisión de la autoridad, de conformidad con el procedimiento «*ANCC-PO-07, Supervisión del cumplimiento*» y en su caso el procedimiento «*ANCC-PO-11, Revisión interpares de la ANCC*».

24. En el ejercicio de sus funciones de supervisión, la **ANCC** podrá solicitar información adicional al **CB** o al titular del certificado, cuando lo considere necesario para verificar la correcta aplicación de los requisitos del esquema **EUCC**.

3.5 COORDINACIÓN CON CSIRT E INTERCAMBIO DE INFORMACIÓN

25. La **ANCC** coordinará, cuando sea necesario y en la medida en que lo exija el marco normativo, con otros agentes. Con carácter general, el **CSIRT** nacional (u otro equipo de respuesta a incidentes competente) solo será informado o implicado cuando la naturaleza de la vulnerabilidad requiera medidas inmediatas de respuesta a incidentes o de protección de la seguridad pública que excedan del ámbito de la certificación. Por ejemplo, si una vulnerabilidad está siendo explotada activamente y supone un riesgo significativo para las personas usuarias o para sistemas críticos, el **JAN** podrá notificar a los **CSIRTs de referencia** nacionales correspondientes a fin de que se adopten medidas de contención o de alerta más amplias. En otros casos, la gestión ordinaria de vulnerabilidades en el marco de la certificación podrá desarrollarse sin intervención directa del **CSIRT**.

3.6 DOCUMENTACIÓN E INFORME

26. Todas las actuaciones realizadas, las decisiones adoptadas y las comunicaciones emitidas o recibidas en el contexto de la gestión de vulnerabilidades se documentarán de manera exhaustiva. La **ANCC** utilizará estos registros para actualizar sus procedimientos internos y para alimentar evaluaciones futuras (por ejemplo, evaluaciones de riesgos para actividades de vigilancia o de recertificación).

27. La **ANCC** elaborará estadísticas e información de síntesis sobre las vulnerabilidades registrada, que formarán parte de sus obligaciones de información anual en virtud del **CSA**. De acuerdo con el «*ANCC-PO-01, Informe anual*», la **ANCC** incluirá en su informe anual dirigido a **ENISA** y al **GECC** datos agregados sobre las vulnerabilidades detectadas en productos certificados y las medidas adoptadas (por ejemplo, número de informes recibidos, número de certificados suspendidos o retirados a causa de vulnerabilidades, etc.), así como las principales actuaciones de coordinación realizadas. Con ello se garantiza la transparencia a escala europea y se permite que el marco europeo de certificación de la ciberseguridad aproveche la experiencia adquirida. Además, los expedientes completos estarán disponibles para la evaluación interpares de la **ANCC** (de conformidad con el artículo 45 del [**EUCC]**) a fin de demostrar que el proceso de gestión de vulnerabilidades de la **ANCC** es sólido y cumple plenamente el **CSA**, el esquema **EUCC** y las directrices de **ENISA** y del **GECC** sobre gestión y divulgación de vulnerabilidades.

4. REFERENCIAS

ACCCB	Acreditación de organismos de certificación para el EUCC (https://certification.enisa.europa.eu/publications/accreditation-cbs-eucc_en)
ACCITSEF	Acreditación de los ITSEF para el EUCC (https://certification.enisa.europa.eu/publications/accreditation-itsefs-eucc_en)
AUTH	Autorización de organismos de certificación e ITSEF para el esquema EUCC (https://certification.enisa.europa.eu/publications/eucc-guidelines-authorisation-cabs_en)
CSA	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 (http://data.europa.eu/eli/reg/2019/881/oj)
CSA-E1	Reglamento (UE) 2025/37 del Parlamento Europeo y del Consejo de 19 de diciembre de 2024 por el que se modifica el Reglamento (UE) 2019/881 en lo que se refiere a los servicios de seguridad gestionados (http://data.europa.eu/eli/reg/2025/37/oj)
EUCC	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 (http://data.europa.eu/eli/reg_impl/2024/482/oj)
LPAC	Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (https://www.boe.es/eli/es/l/2015/10/01/39/con)
NOTIF	Reglamento de Ejecución (UE) 2024/3143 de la Comisión, de 18 de diciembre de 2024, por el que se establecen las circunstancias, los formatos y los procedimientos de notificación con arreglo al artículo 61, apartado 5, del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación (http://data.europa.eu/eli/reg_impl/2024/3143/oj)
VULMD	Directrices sobre gestión y divulgación de vulnerabilidades (https://certification.enisa.europa.eu/publications/eucc-guidelines-vulnerability-management-and-disclosure-and-eccg-opinion_en)

5. ACRÓNIMOS

ANCC	Autoridad Nacional de Certificación de la Ciberseguridad
CCN	Centro Criptológico Nacional
CE	Comisión Europea
CSIRT	Equipos de Respuesta a Incidentes de Seguridad Informática
ENAC	Entidad Nacional de Acreditación
ENISA	Agencia de la Unión Europea para la Ciberseguridad
EUCC	Esquema europeo de certificación de la ciberseguridad basado en criterios comunes
GECC	Grupo Europeo de Certificación de la Ciberseguridad
ITSEF	Instalación de evaluación de la seguridad de las tecnologías de la información
JAN	Jefe de la unidad de la ANCC
OC	Organismo de Certificación
OEC	Organismo de Evaluación de la Conformidad
ONA	Organismo Nacional de Acreditación
PPP	Paquete de preparación de la evaluación por pares
CSA	Reglamento sobre la Ciberseguridad
SED	Secretario de Estado Director del CCN
SGA	Sistema de Información de la Autoridad Nacional de Certificación de la Ciberseguridad
TA	Personal Técnico adscrito a la ANCC
TIC	Tecnologías de la Información y la Comunicación
UE	Unión Europea
WANCC	Sitio web de la Autoridad Nacional de Certificación de la Ciberseguridad