Autoridad Nacional de Certificación de la Ciberseguridad

centro criptológico nacional

ANCC-PO-04

Directrices de cooperación

Marzo de 2026
Versión 1

MINISTERIO DE DEFENSA

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

CONTROL DE VERSIONES

Versión	Comentarios
1.0	Versión inicial

ÍNDICE

1. INTRODUCCIÓN

1. El presente documento define lo siguiente:

   a) Las tareas de cooperación que la Autoridad Nacional de Certificación (**ANCC)** debe llevar a cabo, de acuerdo con la **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], y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad») y el 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].**

   b) Para cada una de estas tareas de coordinación, se debe contar con un procedimiento y una directriz que garanticen su ejecución coherente y repetible, o bien un enlace al procedimiento general de la **ANCC** correspondiente que incluya la tarea de coordinación pertinente.

2. POLÍTICA GENERAL DE COOPERACIÓN

2. La Autoridad Nacional de Certificación **(ANCC)** cooperará con la Agencia de la Unión Europea para la Ciberseguridad **(ENISA)**, el grupo europeo de certificación de la ciberseguridad **(GECC)**, otras **ANCC** y las autoridades nacionales pertinentes de manera oportuna, estructurada y segura, garantizando la confidencialidad, la integridad y la trazabilidad de todos los intercambios.

3. El jefe de la unidad de la **ANCC (JAN)** es responsable de las decisiones de cooperación y de los compromisos externos, mientras que el personal técnico **(TA)** coordina las actividades diarias de cooperación, actúa como punto de contacto único, prepara las aportaciones técnicas y ejecuta los pasos operativos requeridos por este procedimiento.

4. Todos los registros, notificaciones, contribuciones y decisiones de cooperación se registrarán en el Sistema de Información de la Autoridad Nacional de Certificación de la Ciberseguridad **(SGA)**. Cuando la cooperación se relacione con otros procedimientos internos, se consignarán referencias cruzadas (por ejemplo, «*ANCC-PO-02, Asistencia y apoyo al Organismo Nacional de Acreditación*», «*ANCC-PO-03, Autorización de organismos de evaluación de la conformidad*», «*ANCC-PO-09, Notificación de organismos de evaluación de la conformidad*», «*ANCC-PO-01, Informe anual*»).

3. PROCEDIMIENTOS DE IMPLEMENTACIÓN DE LOS REQUISITOS DE COOPERACIÓN

3.1 ARTÍCULO 8(3) DEL REGLAMENTO (UE) 2019/881, CONTRIBUCIÓN A LAS DIRECTRICES Y BUENAS PRÁCTICAS DE ENISA

5. **JAN** recopilará las aportaciones anuales de los **TA** sobre las prácticas nacionales de certificación, los problemas de implementación de los esquemas y los comentarios del sector; **JAN** valida la posición que se facilitará a **ENISA** y, cuando proceda, a las estructuras de trabajo del **GECC**.

6. Participación en consultas y grupos de trabajo de **ENISA**: **TA** asiste a las sesiones, presenta observaciones por escrito y casos de estudio, garantiza el control de versiones y mantiene el registro de envíos en el **SGA**; **JAN** podrá aprobar cualquier posición o postura que adopte la **ANCC**.

7. Integración de resultados: Una vez que **ENISA** publique directrices o buenas prácticas, **TA** analiza su aplicabilidad, registra las decisiones y realiza el seguimiento de las acciones correspondientes; **JAN** decide sobre la adopción y las actualizaciones necesarias de los procedimientos internos en base a las propuestas de los **TA**.

3.2 ARTÍCULO 58(H) DEL REGLAMENTO (UE) 2019/881, INTERCAMBIO DE INFORMACIÓN SOBRE POSIBLE INCUMPLIMIENTO

8. Los eventos desencadenantes incluyen alertas de vigilancia del mercado, reclamaciones, informes de **OC/ITSEF** o investigaciones de la **ANCC**. El **TA** realiza una evaluación inicial y consolida las pruebas; el **JAN** determina si la información justifica el intercambio transfronterizo.

9. Sin demora indebida, **JAN** comparte un aviso con otras **ANCC** (a través del canal seguro del **GECC**) y con las autoridades nacionales pertinentes, incluyendo los hechos esenciales, el producto, servicio o proceso **TIC** afectado, el esquema y el nivel de garantía, así como las acciones sugeridas. Los datos confidenciales o de carácter personal se minimizan y se comparten únicamente sobre la base de la estricta necesidad de conocerlos.

10. Vínculo con otros procedimientos: si el caso afecta a la autorización o supervisión de un Organismo de Evaluación de la Conformidad (**OEC)**, se coordinará con el «*ANCC-PO-03, Autorización de organismos de evaluación de la conformidad*»; si surgen aspectos relacionados con la acreditación, se informará a la Entidad Nacional de Acreditación (**ENAC)** de conformidad con el «*ANCC-PO-02, Asistencia y apoyo al Organismo Nacional de Acreditación*».

3.3 ARTÍCULO 58(9) DEL REGLAMENTO (UE) 2019/881, INTERCAMBIO DE INFORMACIÓN, EXPERIENCIA Y BUENAS PRÁCTICAS

11. El jefe de la unidad (**JAN**) o el personal técnico (**TA**) designado por este participa en las sesiones plenarias y grupos de trabajo del **GECC**; **TA** prepara resúmenes (métricas, lecciones aprendidas y cuestiones técnicas), presenta la experiencia nacional, mantiene un repositorio de las buenas prácticas recibidas y coordina su adopción a escala nacional.

12. Las solicitudes de la Comisión o de otras **ANCC** son registradas y gestionadas por el **TA**; este prepara las respuestas, que son aprobadas por el **JAN**, y todos los intercambios se registran y mantienen actualizados en el **SGA**.

3.4 ARTÍCULO 62(2)(G) DEL REGLAMENTO (UE) 2019/881, APOYO AL GECC EN LA CREACIÓN DE CAPACIDADES Y MÉTODOS DE INTERCAMBIO DE INFORMACIÓN

13. El personal técnico (**TA**) contribuye a la definición y funcionamiento de las herramientas de intercambio de información del **GECC** (portales seguros, formatos, taxonomías) y participa en actividades de creación de capacidades, ya sea como alumno o formador, mientras que el jefe de la unidad de la **ANCC** (**JAN**) aprueba la asignación de recursos.

14. Cuando el **GECC** emita plantillas de cooperación, directrices o documentos de referencia sobre el estado de la técnica, **TA** asegura su integración en este procedimiento y en los flujos de trabajo internos relacionados; los registros de formación se mantienen en el **SGA**.

3.5 ARTÍCULO 7(2) DEL REGLAMENTO DE EJECUCIÓN (UE) 2024/482, EXCEPCIONES A LOS DOCUMENTOS DE ESTADO DE LA TÉCNICA

15. Recepción y registro: el personal técnico de la **ANCC** (**TA**) registra las solicitudes de excepción de los **OEC** con su justificación y la metodología alternativa propuesta, y realiza una evaluación técnica, consultando opcionalmente a expertos externos sujetos a obligaciones de confidencialidad.

16. Decisión e informe: el jefe de la unidad de la **ANCC** (**JAN**) aprueba o rechaza la solicitud; si se aprueba, **TA** notifica sin demora indebida al **GECC** el alcance y la base de la decisión, registra la notificación y cualquier dictamen del **GECC**, y vela por que las condiciones asociadas se apliquen durante la supervisión de la evaluación.

3.6 ARTÍCULO 12(3) DEL REGLAMENTO DE EJECUCIÓN (UE) 2024/482, VALIDEZ DEL CERTIFICADO SUPERIOR A 5 AÑOS

17. Procedimiento de aprobación previa: el **OC** presenta la justificación; **TA** evalúa el ciclo de vida, el panorama de amenazas y las medidas de mantenimiento; **JAN** adopta la

decisión. Tras la aprobación, **TA** notifica al **GECC** e informa a **ENISA** para garantizar la exactitud del repositorio.

18. Seguimiento: **TA** planifica revisiones intermedias o actualizaciones de estado para los certificados de validez ampliada; el seguimiento se registra en el **SGA**.

3.7 ARTÍCULO 14(2) DEL REGLAMENTO DE EJECUCIÓN (UE) 2024/482, NOTIFICACIONES DE RETIRADA DE CERTIFICADOS

19. Tras la notificación de retirada por parte del **OC**, el personal técnico de la **ANCC** (**TA**) registra los detalles; verifica que **ENISA** haya sido informada por el **OC**; prepara y envía las notificaciones a las autoridades nacionales de vigilancia del mercado y, cuando proceda, a los reguladores sectoriales. Opcionalmente, se podrá enviar una notificación de cortesía a otras **ANCC** a través de los canales del **GECC**.

20. Seguimiento de tendencias: **TA** mantiene un registro de las retiradas para identificar posibles problemas sistémicos; se proponen acciones correctoras al jefe de la unidad de la **ANCC** (**JAN**). Se establecen las interfaces oportunas con el «*ANCC-PO-09, Notificación de organismos de evaluación de la conformidad*» cuando proceda.

3.8 ARTÍCULO 25(9) DEL REGLAMENTO DE EJECUCIÓN (UE) 2024/482, INVESTIGACIONES TRANSFRONTERIZAS Y NOTIFICACIÓN AL GECC

21. Cuando las investigaciones afecten a productos **TIC** certificados en otros Estados miembros, **TA** informa a las **ANCC** pertinentes para facilitar la colaboración y notifica asimismo al **GECC** sobre la investigación y los resultados posteriores. **JAN** coordina la interlocución técnica entre las autoridades y los **OC** involucrados.

3.9 ARTÍCULO 38 DEL REGLAMENTO DE EJECUCIÓN (UE) 2024/482, COOPERACIÓN EN MATERIA DE VULNERABILIDADES

22. Tras recibir información sobre vulnerabilidades (de conformidad con el artículo 37 **[EUCC]**), el **JAN** será el encargado compartir la información pertinente con otras **ANCC** y con **ENISA**, y mantiene la confidencialidad hasta que se cumplan las condiciones establecidas para la publicación.

23. Si otra **ANCC** lo solicita, **TA** facilita las evaluaciones por parte de los **OC** nacionales, garantizando que, con carácter previo, se informe al titular del certificado. En los casos excepcionales de certificaciones previstas en el artículo 38, apartado 4, el **JAN** comunica la intención al **GECC** y registra el dictamen emitido.

4. REGISTROS, CONFIDENCIALIDAD Y SEGURIDAD

24. Todos los elementos derivados de la cooperación (aportaciones, notificaciones, correspondencia con el **GECC** y **ENISA**, dictámenes, actas de reuniones) se almacenarán en el **SGA** con un control de acceso y unos períodos de conservación adecuados, de conformidad con las políticas internas de seguridad de la información y los requisitos del esquema.

25. Los documentos compartidos externamente se someten a control de versiones; la información sensible se marca y gestiona de acuerdo con los requisitos de protección de la información establecidos en el artículo 43 del **[EUCC]**, cuando resulte de aplicación.

5. 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)

6. 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
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