Autoridad Nacional de Certificación de la Ciberseguridad

centro criptológico nacional

# ANCC-GU-01

# Descripción general de la Autoridad Nacional de Certificación de la Ciberseguridad

**Marzo de 2026**
**Versión 1**

MINISTERIO DE DEFENSA

## CONTROL DE VERSIONES

| Versión | Comentarios |
|---|---|
| **1.0** | Versión inicial |
| | |

# ÍNDICE

# 1. INTRODUCCIÓN

1. La Secretaria de Estado Directora del Centro Nacional de Inteligencia, como directora del Centro Criptológico Nacional (**CCN**), ha sido designada en España como Autoridad Nacional de Certificación de la Ciberseguridad (**ANCC**) para los esquemas de certificación desarrollados en virtud del **Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA y a la certificación de la ciberseguridad de las TIC** (en adelante, **CSA**, por sus siglas en inglés) **[CSA]** y la implementación nacional de dicho reglamento.

2. Según el artículo 58 del **[CSA]**, cada Estado miembro debe designar una o más autoridades nacionales de certificación de la ciberseguridad. El **CCN**, como oficina de apoyo a la ANCC, se encarga de supervisar y gestionar la implementación de los esquemas de certificación de ciberseguridad en nuestro país.

3. El **CCN** como **ANCC** debe desempeñar las siguientes funciones:

   a) supervisar y velar por la aplicación de las normas recogidas en los esquemas europeos de certificación de la ciberseguridad, para controlar la conformidad de los productos, servicios y procesos de **TIC** con los requisitos de los certificados europeos de la ciberseguridad que hayan sido expedidos en sus respectivos territorios, en cooperación con otras autoridades de vigilancia del mercado pertinentes;

   b) controlar el cumplimiento y la aplicación de las obligaciones de los fabricantes y proveedores de productos, servicios o procesos de **TIC** establecidos en sus respectivos territorios y que llevan a cabo autoevaluaciones de la conformidad, en particular controlar el cumplimiento y la aplicación de las obligaciones de tales fabricantes y proveedores en el correspondiente esquema europeo de certificación de la ciberseguridad;

   c) asistir y apoyar activamente a los organismos nacionales de acreditación en el control y la supervisión de las actividades de los organismos de evaluación de la conformidad a efectos de la aplicación del presente Reglamento;

   d) controlar y supervisar las actividades de los organismos públicos mencionados en el artículo 56, apartado 5 del **[CSA]**;

   e) cuando proceda, autorizar a los organismos de evaluación de la conformidad y restringir, suspender o retirar las autorizaciones en vigor en caso de incumplimiento, por parte de los organismos de evaluación de la conformidad, de los requisitos del **CSA**;

   f) tramitar las reclamaciones presentadas por personas físicas o jurídicas en relación con los certificados europeos de ciberseguridad expedidos por las autoridades nacionales de certificación de la ciberseguridad o los certificados europeos de ciberseguridad expedidos por los organismos de evaluación de la conformidad o, en relación con las declaraciones de conformidad UE, investigar el asunto objeto de la reclamación en la medida que proceda e informar al

reclamante sobre el curso y el resultado de la investigación en un plazo razonable;

g) presentar a la Agencia de la Unión Europea para la Ciberseguridad (**ENISA**) y al Grupo Europeo de Certificación de la Ciberseguridad **(GECC)** un informe sucinto anual de las actividades realizadas con arreglo al **CSA**;

h) cooperar con otras autoridades nacionales de certificación de la ciberseguridad u otras autoridades públicas, en particular mediante el intercambio de información sobre posibles productos, servicios y procesos de **TIC** que no se ajusten a los requisitos del presente Reglamento o de esquemas europeos de certificación de la ciberseguridad específicos, y

i) seguir las novedades de interés en el ámbito de la certificación de la ciberseguridad.

4. Estas responsabilidades son esenciales para garantizar un alto nivel de ciberseguridad y confianza en los productos y servicios digitales dentro de la Unión Europea.

5. Los principales roles y cargos que intervienen en el desempeño del **CCN** como **ANCC** son los siguientes:

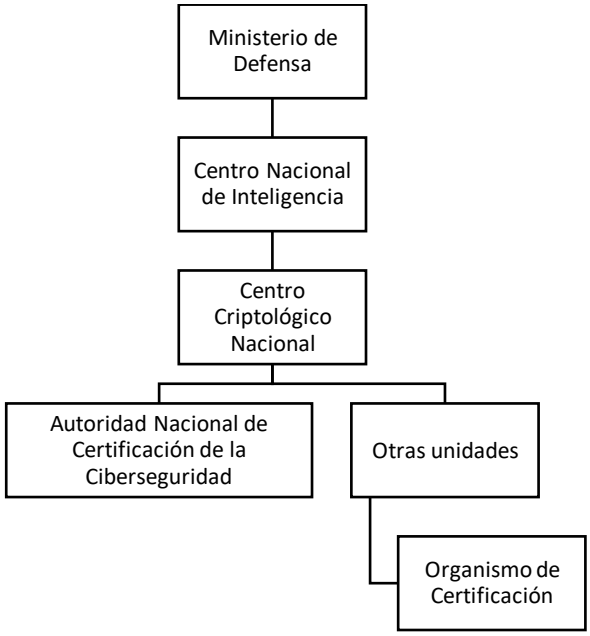
- **SED**: Secretario de Estado Director del CCN
- **SGCCN**: Subdirector General del CCN
- **JAN**: Jefe de la unidad de la ANCC
- **TA**: Personal Técnico adscrito a la ANCC
- **JOC**: Jefe de la unidad del OC

6. Este documento ofrece un breve resumen de la organización y responsabilidades de la **ANCC** en el marco del **CCN**.

## 2. ESTRUCTURA

7. La **ANCC** es una unidad administrativa perteneciente al **CCN**, adscrito al Centro Nacional de Inteligencia (**CNI**) conforme al siguiente diagrama de dependencia orgánica:

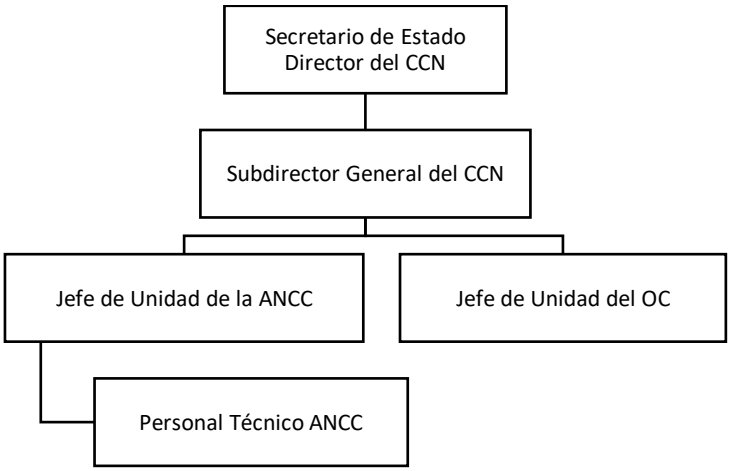
*Figura 1 - Estructura*




8. Los siguientes cargos se definen por el **CCN** para la implementación de la **ANCC**:

a) **SED**, la autoridad de máximo nivel, responsable de la **ANCC**;
b) **SGCCN**, autoridad ejecutiva que gestiona la **ANCC**, rinde cuentas ante **SED**;
c) **JAN**, jefe de la unidad de la **ANCC**, rinde cuentas ante **SGCCN**;
d) **TA**, personal de la **ANCC**, depende de **JAN**;

*Figura 2 - Organigrama*



9. El **CCN** también actúa como un Organismo de Evaluación de la Conformidad (**OEC**) como organismo de certificación (**OC**), en el sentido del **CSA**, operando actualmente en el marco del **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]**, para el nivel de garantía «alto», también denominado **OC**. Este **OC** está autorizado, supervisado y sometido a vigilancia por la **ANCC**.

10. La imparcialidad e independencia entre las actividades de supervisión y certificación como **ANCC** y **OC** respectivamente es tratada en el documento *«CB-001 Análisis de riegos y gestión de la imparcialidad e independencia del OC/ANCC»* donde se establecen los requisitos aplicables a la imparcialidad e independencia del Organismo de Certificación, analizando los riesgos para la imparcialidad e independencia exigida, y estableciendo las condiciones, mecanismos y procedimientos necesarios para mitigar tales riesgos y garantizar el cumplimiento de dichos requisitos, facilitando la correspondencia entre los requisitos y su mecanismo de cumplimiento.

11. Los siguientes cargos se definen por el **CCN** para la implementación del **OC**:

a) **SED**, la autoridad de máximo nivel, responsable del **OC**;
b) **JCCN**, rinde cuentas ante **SED**, autoridad ejecutiva que gestiona el **OC**;
c) **JOC**, jefe de la unidad del **OC**, rinde cuentas ante **JCCN**.

## 3. DOCUMENTACIÓN

12. Los procedimientos operativos de la **ANCC** se definen en los documentos siguientes:

| Identificador | Título |
|---|---|
| **ANCC-GU-01** | Descripción general de la Autoridad Nacional de Certificación de la Ciberseguridad |
| **ANCC-PO-01** | Informe anual |
| **ANCC-PO-02** | Asistencia y apoyo al Organismo Nacional de Acreditación |
| **ANCC-PO-03** | Autorización de organismos de evaluación de la conformidad |
| **ANCC-PO-04** | Directrices de cooperación |
| **ANCC-PO-05** | Gestión de reclamaciones |
| **ANCC-PO-06** | Autorización para el uso de la marca CCRA |
| **ANCC-PO-07** | Supervisión del cumplimiento |
| **ANCC-PO-08** | Seguimiento de novedades en certificación de ciberseguridad |
| **ANCC-PO-09** | Notificación de organismos de evaluación de la conformidad |
| **ANCC-PO-10** | Evaluación interpares |
| **ANCC-PO-11** | Revisión interpares de la Autoridad Nacional de Certificación de la Ciberseguridad |
| **ANCC-PO-12** | Recepción de certificados y declaraciones de conformidad |
| **ANCC-PO-13** | Gestión de vulnerabilidades |

# 4. VISIÓN GENERAL DE LOS ASPECTOS OPERATIVOS

## 4.1 SERVICIOS TRAMITADOS COMO PROCEDIMIENTOS ADMINISTRATIVOS PÚBLICOS

### 4.1.1 NOTIFICACIÓN DE OEC

13. A la **ANCC** le corresponde notificar oficialmente a la Comisión Europea (**CE**) los **OEC** acreditados (y, en su caso, autorizados) para expedir certificados en virtud de cada esquema europeo de certificación de la ciberseguridad de acuerdo al **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 [NOTIF].** Esta notificación garantiza el reconocimiento de dichos **OEC** a nivel europeo: aproximadamente un año después de la entrada en vigor de un esquema, la Comisión publica en el Diario Oficial de la Unión Europea (**UE**) una lista de los **OEC** notificados, basada en la información proporcionada por la **ANCC** de cada Estado miembro.

14. Además, la **ANCC** debe informar sin demora a la Comisión de cualquier cambio en la situación de un **OEC** —como nuevas autorizaciones, suspensiones o retiradas— a fin de que el registro oficial de organismos de evaluación de la conformidad de la **UE** se mantenga actualizado. Las notificaciones se presentan a través de un sistema electrónico designado según lo especificado por la **CE**. En España, el acto de notificar un **OEC** se tramita como un procedimiento administrativo, lo que implica que sigue pasos formales. Para más detalles, véase el procedimiento «*ANCC-PO-09, Notificación de organismos de evaluación de la conformidad*».

### 4.1.2 AUTORIZACIÓN DE OEC

15. La **ANCC** es responsable de autorizar a los OEC a operar en el marco de los esquemas europeos de certificación de la ciberseguridad en los niveles de garantía correspondientes (en particular para esquemas de nivel "alto" como el **EUCC**). Antes de conceder una autorización, la **ANCC** verifica que un **OEC** candidato esté debidamente acreditado por la Entidad Nacional de Acreditación (**ENAC**) para el alcance pertinente y que cumpla cualquier requisito adicional específico del esquema definido en el marco europeo. Una vez autorizado, un **OEC** queda facultado formalmente para expedir certificados en el marco del esquema, y la **ANCC** notificará este estatus a la **CE**. La **ANCC** también mantiene la facultad de restringir, suspender o retirar una autorización si el **OEC** incumple sus obligaciones o si su competencia se pone en duda, lo que garantiza que solo los organismos cualificados y conformes puedan seguir expidiendo resultados certificados. Este procedimiento de autorización se describe en el procedimiento «*ANCC-PO-03 Autorización de organismos de evaluación de la conformidad*».

### 4.1.3 GESTIÓN DE RECLAMACIONES

16. La **ANCC** mantiene un procedimiento formal para gestionar las reclamaciones de fabricantes, proveedores de servicios u otras partes interesadas en relación con las certificaciones de ciberseguridad y las autoevaluaciones de conformidad de la **UE**. Estas reclamaciones pueden referirse, por ejemplo, a un certificado europeo expedido por la **ANCC** o por un **OEC** acreditado, o a cuestiones relacionadas con una declaración **UE** de conformidad. Al recibir una reclamación, la **ANCC** lleva a cabo la investigación pertinente y mantiene informado al reclamante sobre el progreso y el resultado. Este proceso garantiza la rendición de cuentas en el sistema de certificación y proporciona un mecanismo para abordar las preocupaciones sobre productos certificados o la conducta de los **OEC**. Cabe destacar que los hallazgos de las reclamaciones también pueden suponer la supervisión más amplia de la **ANCC** (por ejemplo, una reclamación fundamentada sobre un **OEC** o un certificado puede desencadenar un escrutinio adicional o acciones correctivas en el marco de los procedimientos de vigilancia de la **ANCC**). Para más detalles, véase el procedimiento «*ANCC-PO-05, Gestión de reclamaciones*».

### 4.1.4 RECEPCIÓN Y REGISTRO DE CERTIFICADOS

17. La **ANCC** se asegura de que todos los certificados de ciberseguridad emitidos al amparo de esquemas europeos en España sean debidamente recibidos por la autoridad y registrados en su registro nacional. Siempre que un **OEC** notificado y/o autorizado emite un nuevo certificado (por ejemplo, bajo el esquema **EUCC**), la **ANCC** puede requerir que el **OEC** notifique o remita los detalles del certificado al sistema de información de la **ANCC**. Mantener actualizado este registro permite a la **ANCC** realizar un seguimiento de los productos y servicios certificados a efectos de supervisión.

18. Además, como parte del reconocimiento mutuo del marco europeo, la **ANCC** acepta los certificados emitidos por **OEC** de otros Estados miembros como válidos a nivel nacional sin pasos de certificación adicionales. La **ANCC** registra tales certificados entrantes y los incorpora en las actividades nacionales de vigilancia del mercado (asegurando, por ejemplo, que los reguladores y usuarios españoles conozcan estos productos certificados). En efecto, la **ANCC** actúa como punto de contacto nacional y centro de intercambio para todos los certificados europeos de ciberseguridad en su territorio, facilitando su reconocimiento y seguimiento. Para más detalles, véase el procedimiento «*ANCC-PO-12, Recepción de certificados y declaraciones de conformidad*».

### 4.1.5 GESTIÓN DE VULNERABILIDADES

19. La **ANCC** coordina un proceso para gestionar y divulgar las vulnerabilidades encontradas en productos, servicios, procesos TIC o servicios de seguridad gestionados certificados bajo esquemas europeos de ciberseguridad. Si se notifica una vulnerabilidad de seguridad significativa, la **ANCC** colabora con el **OEC** emisor y los

equipos **CSIRT** pertinentes para garantizar que el fabricante del producto sea informado y que se tomen medidas de subsanación en tiempo oportuno.

20. Las políticas específicas de cada esquema (por ejemplo, directrices del esquema **EUCC**) definen el papel de la **ANCC** en la divulgación coordinada de vulnerabilidades. La **ANCC** puede facilitar la comunicación entre los investigadores de seguridad, el fabricante afectado y el **OEC**, supervisar el progreso de la mitigación de la vulnerabilidad y, de ser necesario, tomar medidas como asesorar sobre el estado o las condiciones del certificado hasta que se resuelva el problema. Al integrar esta gestión de vulnerabilidades en el ciclo de vida de la certificación, la **ANCC** contribuye a preservar la confianza en los productos certificados incluso ante nuevas amenazas, asegurando que las incidencias de seguridad posteriores a la certificación se gestionen de manera responsable. Para más detalles, véase el procedimiento «*ANCC-PO-13, Gestión de vulnerabilidades*».

### 4.1.6 AUTORIZACIÓN Y SUPERVISIÓN PARA EL USO DE LA MARCA CCRA EN EL ESQUEMA EUCC

21. El procedimiento «*ANCC-PO-06, Procedimiento de autorización y supervisión para el uso de la marca CCRA en el esquema EUCC*» establece el marco mediante el cual la **ANCC** autoriza y supervisa el uso de la marca **CCRA** en certificados emitidos bajo el esquema **EUCC** por organismos de certificación (**CBs**) que no son firmantes del acuerdo internacional. El proceso se articula como un procedimiento administrativo simplificado conforme a la Ley 39/2015 e integra una revisión documental inicial, la apertura de expediente, la supervisión técnica exhaustiva de cada certificación y, finalmente, una resolución motivada que puede autorizar o denegar el uso de la marca. Su objetivo es asegurar que los certificados emitidos mantengan el rigor, trazabilidad y alineamiento metodológico exigidos por el **CCRA**, preservando así su reconocimiento y validez internacional.

    Asimismo, el procedimiento define las obligaciones que deben asumir los **CBs** para mantener la autorización, incluyendo la participación en las *Voluntary Periodic Assessments* (**VPA**) del **CCRA**, la entrega completa de la documentación técnica, la cooperación con la **ANCC** y con los equipos auditores internacionales, la disponibilidad del personal técnico y la implantación de acciones correctivas cuando proceda. El incumplimiento de estas obligaciones puede derivar en la suspensión o retirada del uso de la marca **CCRA**. En conjunto, el procedimiento garantiza que cualquier organismo autorizado opere con un nivel de exigencia equivalente al de los esquemas gubernamentales firmantes del acuerdo, reforzando la confianza y consistencia del ecosistema de certificación europeo

## 4.2 APOYO AL ORGANISMO NACIONAL DE ACREDITACIÓN

22. La **ANCC** apoya activamente a la Entidad Nacional de Acreditación **(ENAC)** en la acreditación de los organismos de evaluación de la conformidad en ciberseguridad. Esta colaboración incluye proporcionar conocimientos técnicos y orientación específicos del esquema durante los procesos de acreditación —por ejemplo, la **ANCC**

puede asignar **TA** cualificado para asistir a **ENAC** en la evaluación de **OEC** candidatos para esquemas europeos. La **ANCC** también comparte información con **ENAC** sobre el desempeño y cumplimiento de los **OEC** acreditados (obtenida de las propias actividades de supervisión de la **ANCC**) para garantizar que cualquier problema sea reconocido y abordado en el contexto de la acreditación. Trabajando estrechamente en consonancia con el artículo 58(c) del **[CSA]**, la **ANCC** y el **ENAC** ayudan a mantener un alto nivel de competencia entre los **OEC** acreditados y agilizan el camino desde la acreditación hasta la autorización (por ejemplo, los resultados de evaluaciones técnicas obtenidos con el apoyo de la **ANCC** pueden utilizarse como evidencias cuando esos **OEC** solicitan la autorización de la ANCC). Para más detalles, véase el procedimiento «*ANCC-PO-02, Asistencia y apoyo al Organismo Nacional de Acreditación*».

## 4.3 COOPERACIÓN E INTERCAMBIO DE INFORMACIÓN

23. La **ANCC** coopera con otras autoridades nacionales de certificación de la ciberseguridad y con instituciones europeas para armonizar prácticas y compartir información crítica. Participa en el Grupo Europeo de Certificación de la Ciberseguridad (**GECC**), donde interactúa con la **CE** y con sus **ANCCs** homólogas de otros países para intercambiar experiencias, debatir casos de incumplimiento o riesgos emergentes, y desarrollar enfoques coordinados. Mediante dicha cooperación (según lo previsto en el artículo 58(h) del **[CSA]**), la **ANCC** contribuye a una aplicación coherente de los esquemas de certificación en todos los Estados miembros y ayuda a posibilitar respuestas conjuntas a los desafíos de ciberseguridad transfronterizos. La información procedente de las propias actividades de la **ANCC** (por ejemplo, hallazgos significativos de supervisión o mejores prácticas) se comparte según corresponda en estos foros, fomentando la alineación y la mejora continua a nivel europeo. Para más detalles, véase el procedimiento «*ANCC-PO-04, Directrices de cooperación*».

## 4.4 SUPERVISIÓN DEL CUMPLIMIENTO Y EJECUCIÓN

24. La **ANCC** supervisa de forma continua el cumplimiento de los certificados emitidos, de los productos o servicios **TIC** certificados, y de las actividades de los **OEC** notificados y autorizados, para garantizar la adhesión continua a las normas de cada esquema de certificación de la ciberseguridad. Emplea mecanismos como la exigencia de informes periódicos de los **OEC**, la revisión de muestras de productos certificados o documentación, y la realización de sus propias auditorías o investigaciones.

25. Si se detecta algún incumplimiento o deficiencia de seguridad —por ejemplo, si se determina que un producto certificado ya no cumple los criterios de seguridad requeridos o si un **OEC** incumple sus obligaciones— la **ANCC** tiene la facultad de tomar medidas coercitivas. Puede requerir información o medidas correctivas, coordinarse con las autoridades de vigilancia del mercado, y en casos graves retirar o invalidar los certificados afectados y suspender o revocar la autorización del **OEC** responsable. Estas facultades (otorgadas por el **CSA** y la legislación nacional) permiten a la **ANCC** preservar la credibilidad del marco de certificación. Al garantizar de esta manera el

cumplimiento, la **ANCC** ayuda a mantener la confianza en los certificados emitidos bajo su supervisión. Para más detalles, véase el procedimiento «*ANCC-PO-07, Supervisión del cumplimiento*».

## 4.5 EVALUACIÓN INTERPARES

26. Bajo ciertos esquemas europeos —en especial el esquema **EUCC** para certificaciones de nivel alto— los organismos de certificación autorizados se someten a evaluaciones interpares periódicas por expertos de otros países. La **ANCC** facilita estos procesos de evaluación interpares para cualquier **OEC** de nivel alto bajo su supervisión, coordinándose con el cronograma del **GECC** (que tiene como objetivo que cada OEC relevante sea evaluado al menos cada cinco años).

27. Durante una evaluación interpares, un equipo formado por otros organismos de certificación diferentes al evaluado, examinan los procedimientos, la competencia técnica y los expedientes de certificación pasados del organismo de certificación evaluado (a menudo mediante revisión de documentación y visitas in situ), y luego emite un informe con hallazgos y recomendaciones. La **ANCC** se asegura de que el **OEC** brinde plena cooperación y de que cualquier recomendación o mejora necesaria resultante se implemente. Estas evaluaciones interpares específicas de esquema complementan la propia supervisión de la **ANCC** y contribuyen a la calidad coherente de las certificaciones en toda Europa. Para más detalles, véase el procedimiento *«ANCC-PO-10, Evaluación interpares»*.

## 4.6 REVISIÓN INTERPARES

28. La propia **ANCC** está sujeta a revisiones interpares periódicas organizadas por la **CE** y el **GECC** para evaluar su desempeño como autoridad nacional de certificación, según lo establecido en el **reglamento de Ejecución (UE) 2025/2540 de la Comisión, de 9 de diciembre de 2025, por el que se establecen disposiciones de aplicación del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo en lo que respecta al establecimiento de un plan para las revisiones [REV]**. Normalmente realizadas cada pocos años (al menos una vez cada cinco años), estas revisiones implican un equipo multinacional de expertos de otros Estados miembros que examinan cómo la **ANCC** lleva a cabo sus funciones —por ejemplo, cómo supervisa a los **OEC**, hace cumplir los requisitos del esquema, gestiona las reclamaciones e interactúa con otras autoridades.

29. La **ANCC** se prepara para cada revisión interpares proporcionando una amplia documentación de sus procedimientos y cooperando plenamente con el equipo revisor. Recíprocamente, la **ANCC** también contribuye al sistema enviando a sus propios expertos para revisar interpares a las autoridades de otros países, intercambiando así mejores prácticas. Tras una revisión, los hallazgos y cualquier recomendación de mejora se discuten en el seno del **GECC**, y se espera que la **ANCC** los aborde, reforzando sus procesos según sea necesario. Este mecanismo de revisión inter pares mutua ayuda a garantizar estándares elevados y armonizados de supervisión en todas las autoridades nacionales de certificación de la ciberseguridad

de la **UE**. Para más detalles, véase el procedimiento «*ANCC-PO-11, Revisión interpares de la ANCC*».

## 4.7 SEGUIMIENTO DE NOVEDADES

30. Cada año, la **ANCC** elabora un informe anual de resumen de sus actividades de supervisión y certificación, que se remite a **ENISA** y al **GECC** en el primer trimestre del año siguiente. Este informe, exigido por el **[CSA]**, abarca las áreas clave de la labor de la **ANCC** —incluyendo la supervisión de los **OEC**, la asistencia proporcionada a **ENAC**, las decisiones de autorización, y cualquier actividad de evaluación o revisión interpares que haya tenido lugar—. Proporciona tanto datos cuantitativos (p. ej., número de auditorías, acciones de apoyo, autorizaciones) como análisis cualitativos (como tendencias observadas, problemas y recomendaciones de mejora) de las actividades del año. A través de este informe anual, la **ANCC** contribuye a la supervisión a nivel europeo y al intercambio de mejores prácticas, ya que los informes nacionales agregados ayudan a informar los debates y los esfuerzos de armonización en el seno del **GECC**. Para más detalles, véase el procedimiento «*ANCC-PO-01, Informe anual*».

## 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) |
| REV | Reglamento de Ejecución (UE) 2025/2540 de la Comisión, de 9 de diciembre de 2025, por el que se establecen disposiciones de aplicación |

del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo en lo que respecta al establecimiento de un plan para las revisiones interpares (http://data.europa.eu/eli/reg_impl/2025/2540/oj)

## 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 |
| 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 |
| VPA | Auditorías periódicas voluntarias |
| WANCC | Sitio web de la Autoridad Nacional de Certificación de la Ciberseguridad |