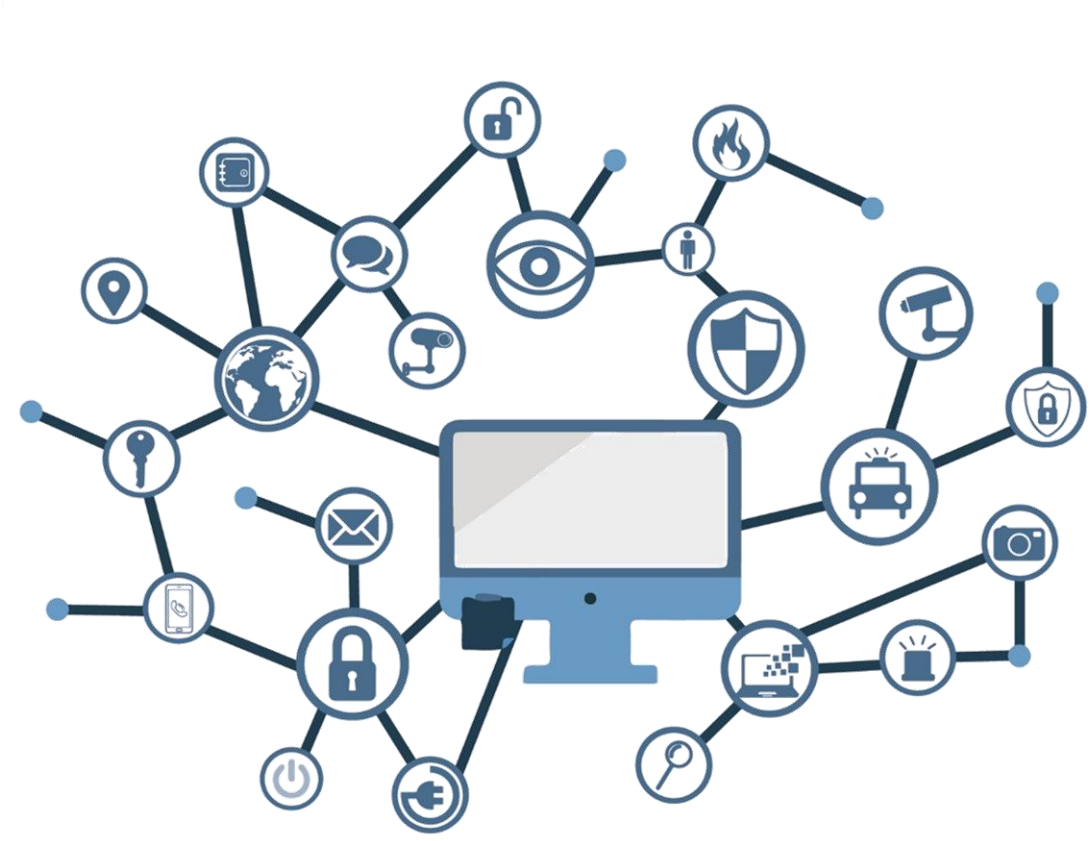
Autoridad Nacional de Certificación de la Ciberseguridad

centro criptológico nacional

ANCC-PO-10

Evaluación interpares



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 establece la política y las normas aplicables a la realización de evaluaciones interpares (*peer assessments*) aplicables a los organismos de certificación que emitan certificados **EUCC** con nivel de aseguramiento «alto», así como a los correspondientes laboratorios de evaluación asociados (**ITSEFs**), conforme a requisitos del **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 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]**.

2. Los organismos de certificación (**OC**) autorizados para emitir certificados EUCC en el nivel de garantía elevado, así como los **ITSEF** asociados que participen en las actividades de evaluación correspondientes, deben someterse periódicamente a evaluaciones interpares conforme a lo establecido en **[CSA]** y en el esquema EUCC. La superación satisfactoria de estas evaluaciones constituye un requisito indispensable para mantener la autorización para operar en el nivel elevado. El objetivo de estas evaluaciones es verificar que los **OEC** evaluados cumplen con los requisitos aplicables del esquema, garantizando que todos los organismos autorizados trabajan de manera armonizada, aplican criterios coherentes y producen certificados del mismo nivel de calidad.

2. POLÍTICA

4. La Autoridad Nacional de Certificación de la Ciberseguridad (**ANCC**) se compromete a facilitar las evaluaciones interpares es para los organismos de certificación que expidan certificados **EUCC** con un nivel de garantía «elevado» y, cuando proceda, para las **ITSEF** relacionadas, de conformidad con los artículos 45 a 47 del **[EUCC]** y con el mecanismo de evaluación interpares establecido en el seno del Grupo Europeo de Certificación en Ciberseguridad (**GECC**).

5. Este compromiso se concreta en:

   a) **Planificación de recursos:** El jefe de la unidad de la **ANCC (JAN)** vela por que exista un número suficiente de personal técnico de la **ANCC (TA)** formados y disponibles para apoyar la planificación, coordinación y ejecución de las evaluaciones interpares, incluida la entrega puntual de información y el apoyo presencial a los equipos de evaluación interpares.

   b) **Colaboración:** el **JAN** mantiene una estrecha cooperación con los **OC** evaluados y sus **ITSEF**, con el **GECC y con ENISA,** a fin de que las evaluaciones se desarrollen de manera eficaz, armonizada e imparcial.

   c) **Independencia y separación de funciones:** cuando el Centro Criptológico Nacional (**CCN)** actúe también como **OC,** la **ANCC** garantizará una estricta separación entre su papel de supervisión y coordinación en la evaluación interpares y cualquier función operativa en las actividades de certificación, asegurando la imparcialidad.

   d) **Seguridad de la información y confidencialidad:** el **JAN** impondrá medidas de seguridad, confidencialidad y protección de datos personales para toda la información relativa a evaluaciones interpares, utilizando el Sistema de Información de la Autoridad Nacional de Certificación de la Ciberseguridad **(SGA)** y canales de intercambio seguros acordados con el equipo de evaluación interpares.

   e) **Transparencia y garantías procedimentales:** el **JAN** se asegurará de que los **OC** evaluados estén informados de las expectativas, plazos y criterios de aceptación, respetando al mismo tiempo el calendario y los procedimientos del **GECC**; las decisiones relevantes se formalizarán con la firma del Secretario de Estado director del CCN **(SED).**

6. Asignación de responsabilidades:

   a) Subdirector General del **CCN** (**SGCCN)** firma las cartas formales, los compromisos de confidencialidad y las comunicaciones finales dirigidas a los organismos de certificación evaluados y al **GECC**.

   b) **JAN** es informado del calendario de evaluaciones interpares, de los principales hitos y de los resultados.

c) **JAN** aprueba la asignación de recursos, la aceptación de los expedientes sometidos a evaluación, las respuestas a los hallazgos y coordina todas las actuaciones de la relacionadas con la evaluación interpares.

d) **TA** designado por el **JAN,** dirige la coordinación específica para el equipo de evaluación interpares, actúa como punto de contacto con el **GECC** y con los organismos de certificación, valida el alcance técnico y la idoneidad de los expedientes y organiza la logística in situ.

e) **TA** apoyan la recopilación de evidencias, el control documental, la transferencia segura de información, la organización de reuniones y el mantenimiento de los registros en el Sistema de Información de la Autoridad Nacional de Certificación de la Ciberseguridad **(SGA)**.

3. NORMAS DE EVALUACIÓN INTERPARES

7. Las evaluaciones interpares se llevarán a cabo exclusivamente de conformidad con los procedimientos aprobados en el seno del **GECC**, que pueden definir la composición del equipo, las fases, la reutilización de evidencias y la elaboración de informes, según lo descrito en los artículos 45 a 47 y en el anexo VI del **[EUCC]**. El **TA** velará por la alineación con las decisiones más recientes del **GECC** e informará al organismo de certificación evaluado de cualquier instrucción de alcance de esquema que afecte a la evaluación.

8. Una vez definido el calendario de evaluación interpares establecido por el **GECC** en coordinación con la **ANCC**, el **OC** evaluado presentará a la **ANCC** un plan de evaluación para su aprobación. El plan incluirá, como mínimo:

    a) El alcance y los objetivos de la evaluación tal como hayan sido comunicados por el **GECC** (incluidos los ámbitos técnicos y, cuando proceda, las **ITSEF** asociadas);

    b) Una propuesta de decisiones de certificación candidatas y de los expedientes de evaluación subyacentes (expedientes de certificación o evaluación) representativos del alcance que vaya a ser muestreado por el equipo de evaluación interpares, junto con una justificación de dicha representatividad;

    c) La clasificación y el marcado de confidencialidad de cada elemento del expediente, propuestas de minimización de datos (por ejemplo, supresiones o acceso exclusivo in situ) y las medidas de tratamiento seguro;

    d) Los plazos propuestos, las restricciones de acceso (por ejemplo, normas aplicables a los laboratorios) y los puntos de contacto designados;

    e) Las declaraciones sobre conflictos de intereses del personal que vaya a interactuar con el equipo de evaluación interpares.

9. El **TA** revisará el plan de evaluación interpares para comprobar su integridad, la idoneidad técnica y el cumplimiento de los requisitos de seguridad y confidencialidad; el **JAN** lo aprobará o solicitará las modificaciones que procedan. La **ANCC** se compromete a facilitar la evaluación interpares y colaborará con el **OC** evaluado para acordar un plan que permita una evaluación eficaz al tiempo que proteja la información sensible, reservada y los datos personales. Cuando exista contenido especialmente sensible, el **TA** podrá autorizar el acceso exclusivamente in situ, la supresión de detalles no esenciales o un muestreo limitado, garantizando que tales medidas no menoscaben los objetivos de la evaluación.

3.1 PREPARACIÓN Y COORDINACIÓN CON EL GECC

10. A la recepción del calendario establecido por el **GECC**, la **ANCC**:

    a) Registrará el plan en el **SGA** y notificará al **OC** evaluado y, en su caso, a las **ITSEF** afectadas;

b) Designará un equipo de coordinación formado por **TA** y nombrará a un responsable de la evaluación;

c) Confirmará con el equipo de evaluación interpares los canales seguros y los procedimientos de intercambio de información;

d) Ajustará el calendario interno a los hitos del **GECC** y comunicará las posibles restricciones o normas aplicables a las visitas.

e) Proporcionará al **GECC** para su valoración, el plan de evaluación propuesto por el **OC** en coordinación con los **ITSEFs.**

3.2 APOYO A LA EJECUCIÓN Y SUMINISTRO DE INFORMACIÓN

11. Durante las fases preparatoria y de visita in situ, el **TA**:

a) Organizará entrevistas con el personal del **OC** evaluado y, cuando proceda, con los **ITSEFs**;

b) Facilitará las visitas a los laboratorios y las demostraciones cuando los ámbitos técnicos entren dentro del alcance de la evaluación;

c) Garantizará que toda la información se trate de conformidad con las medidas de confidencialidad acordadas y se registre en el **SGA**.

12. El **TA** se asegurará de que el equipo de evaluación por pares sea informado sin demora de cualquier cambio sustancial (por ejemplo, en el personal, los procesos o el alcance) que se produzca en el **OC** evaluado o en la **ITSEF** relacionada durante el período de evaluación.

3.3 RESULTADOS, GESTIÓN DEL INFORME Y SEGUIMIENTO

13. Tras la recepción del borrador de informe de evaluación interpares, el **TA** coordinará la elaboración, por parte del **OC** evaluado, el tratamiento de desviaciones y en su caso el plan de acciones correctivas, garantizando su presentación dentro de los plazos fijados por el equipo de evaluación interpares. El **JAN** aprobará la respuesta antes de su envío. El **SGCCN** firmará, cuando proceda, las cartas formales de remisión al **GECC**.

14. Cuando el **GECC** emita su dictamen definitivo, el **TA** registrará el resultado (positivo o negativo, lista de no conformidades, plazos) en el **SGA** y activará, cuando proceda:

a) El seguimiento de las acciones correctivas por parte del **OC** evaluado y, en su caso, de la **ITSEF**;

b) La coordinación con **ENAC** cuando los resultados puedan afectar a la acreditación;

c) La revisión del estado de la autorización con arreglo al «*ANCC-PO-03, Autorización de organismos de evaluación de la conformidad*»;

d) Cualquier actividad de supervisión o control de acuerdo con el «*ANCC-PO-07, Supervisión del cumplimiento*».

15. Los aspectos relativos a la publicación (a cargo de **ENISA**) se apoyarán proporcionando, cuando sea necesario, versiones depuradas de la documentación, garantizando que la información sensible, personal o de carácter propietario se elimine de conformidad con el artículo 47, apartado 6, del **[EUCC].**

3.4 CONFIDENCIALIDAD, SEGURIDAD Y REGISTROS

16. El **JAN** se asegurará de que toda la información relativa a evaluaciones interpares se trate bajo compromisos de confidencialidad adecuados. El **TA** definirá las instrucciones de tratamiento (clasificación, conservación, control de acceso, plazos de conservación y destrucción) y exigirá que los intercambios de expedientes se realicen mediante medios seguros acordados mutuamente. Los **TA** mantendrán registros completos de las comunicaciones, remisiones, asistencias y accesos, a fin de garantizar la trazabilidad y posibilitar auditorías posteriores.

3.5 REUTILIZACIÓN DE EVIDENCIAS

17. El **TA** podrá proponer al equipo de evaluación interpares la reutilización de evidencias recientes de evaluaciones interpares (no anteriores a cinco años) o de procedimientos equivalentes, identificando con precisión su origen, alcance y procedimientos utilizados, de manera que el informe de evaluación interpares pueda especificar los resultados reutilizados con o sin evaluación adicional.

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 interpares
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
SGCCN	Subdirector General del CCN
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