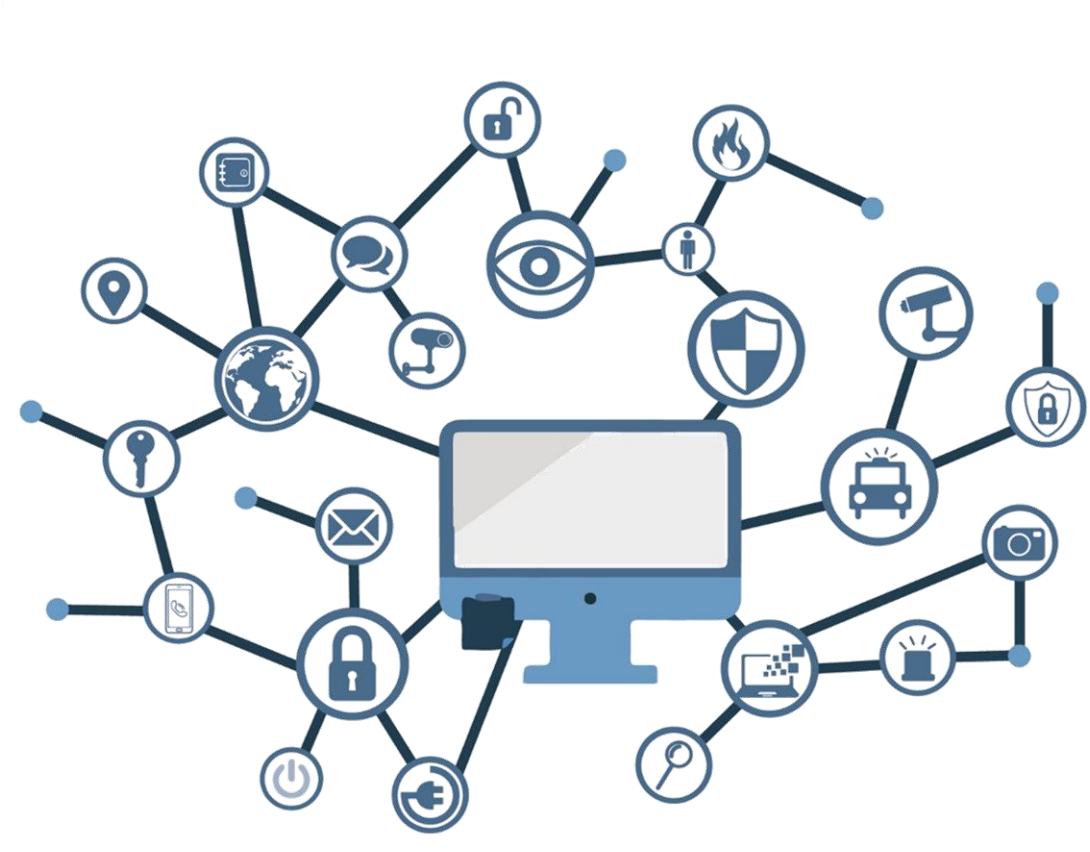
Autoridad Nacional de Certificación de la Ciberseguridad

centro criptológico nacional

ANCC-PO-08

Seguimiento de novedades en certificación de ciberseguridad



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:

   a) El proceso y el procedimiento mediante los cuales la Autoridad Nacional de Certificación **(ANCC**) monitoriza y examina los desarrollos relevantes en el ámbito de la certificación de la ciberseguridad;

   b) La distribución del resultado de este proceso, en forma de informe anual, destinado a contribuir a la mejora de la competencia técnica y capacidades de la propia **ANCC**, de los esquemas 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 de sus partes interesadas.

2. CONTENIDO Y ALCANCE DEL INFORME DE SEGUIMIENTO

2. La **ANCC** monitoriza los desarrollos en diversas áreas a fin de dar cumplimiento a su mandato con arreglo al **[CSA]**, y los refleja en un **informe anual interno de seguimiento de desarrollos**. Este informe interno, destinado a la mejora continua del funcionamiento de la Autoridad, se estructura para incluir, al menos, las secciones siguientes:

a) **Actualizaciones legislativas y reglamentarias** — Resumen de leyes nuevas y/o modificadas, reglamentos o políticas a nivel de la Unión (incluidas las actualizaciones o la nueva normativa adoptada en el marco del **[CSA]**) y a nivel internacional, que sean relevantes para la certificación de la ciberseguridad, junto con un análisis de su impacto potencial en el marco nacional de certificación;

b) **Desarrollos en normas y criterios técnicos** — Novedades relevantes en los organismos de normalización o actualizaciones de criterios técnicos relacionados con la certificación de la ciberseguridad. Esta sección abarca nuevas normas o normas revisadas y directrices (por ejemplo, metodologías de evaluación o requisitos de seguridad) y evalúa cómo pueden influir en las prácticas de certificación o en el reconocimiento de certificados;

c) **Actividades en otras ANCC** — Información sobre iniciativas significativas, cambios procedimentales o buenas prácticas comunicadas por las **ANCC** de otros Estados miembros. Estos desarrollos se recopilan normalmente a través de intercambios en el Grupo Europeo de Certificación de la Ciberseguridad **(GECC)** o de comunicaciones bilaterales, y se examina su relevancia para los propios procedimientos de la Autoridad o para posibles esfuerzos de armonización;

d) **Resultados de conferencias y talleres** — Conclusiones clave de conferencias, talleres o reuniones de grupos de trabajo sobre certificación de la ciberseguridad (por ejemplo, conferencias internacionales de *Common Criteria* o eventos organizados por **ENISA**). Esta sección recoge las tendencias emergentes, recomendaciones o acciones acordadas en estos foros que puedan afectar a los esquemas de certificación o a las técnicas de evaluación;

e) **Investigación y alertas de seguridad** — Conclusiones relevantes de investigaciones académicas, informes del sector o avisos técnicos (por ejemplo, sobre nuevas vulnerabilidades, el panorama de amenazas o tecnologías de seguridad) que puedan afectar a los criterios de certificación o a la garantía de los productos certificados. El informe analiza cómo esta información puede hacer necesario actualizar los esquemas de certificación o los procesos de evaluación; En cada sección, el informe interno no solo documenta los desarrollos, sino que también comenta su importancia y, cuando proceda, formula recomendaciones de actuación (por ejemplo, actualización de directrices, necesidades de formación para el personal técnico de la **ANCC** (**TA**) o ajustes en las prácticas de supervisión). Asimismo, se elabora una versión pública depurada de este informe, en la que se omite cualquier análisis sensible

o de carácter estrictamente interno, manteniendo la información esencial sobre los desarrollos para su comunicación a las partes interesadas externas.

3. PROCESO DE ELABORACIÓN Y REVISIÓN

3. El seguimiento de los desarrollos en la certificación de la ciberseguridad es una actividad continua a lo largo de todo el año, que se formaliza mediante un informe interno anual. El proceso de recopilación de información y de elaboración de dicho informe interno comprende las etapas siguientes:

a) **Recopilación continua de información** — **TA** realiza un seguimiento periódico de las fuentes de información definidas a lo largo del año. En particular, monitoriza las publicaciones oficiales en busca de cambios legislativos y reglamentarios, participa o revisa los resultados de los comités de normalización, sigue las comunicaciones de otras **ANCC** (a menudo a través de la red del **GECC**) y asiste o revisa la documentación de conferencias relevantes. También se centra específicamente en los desarrollos relacionados con los esquemas europeos de certificación de la ciberseguridad (como actualizaciones o directrices relativas al **Reglamento de Ejecución (UE) 2024/482 [EUCC]** u otros esquemas en el marco del **CSA**) y en las publicaciones pertinentes de **ENISA** o en los avisos del **GECC**;

b) **Inicio de la elaboración del informe** — Hacia finales de cada año, el jefe de la unidad de la **ANCC (JAN)** inicia la preparación del informe anual de seguimiento. El **JAN** dirige instrucciones al personal técnico del **ANCC (TA)** para que consoliden todos los desarrollos significativos identificados durante el año. Se establece un calendario (normalmente a comienzos del año siguiente) para la redacción del informe, garantizando la inclusión de los desarrollos de final de año. En esta fase, el **JAN** también puede señalar áreas de interés o preocupación que deban tratarse en el informe;

c) **Redacción del informe** — **TA** prepara un borrador del informe interno de seguimiento de desarrollos. El borrador se estructura conforme a las secciones predefinidas (legislación, normas, otras actividades de **ANCC**, eventos, investigación, etc.), recopilando la información obtenida. Para cada desarrollo o conjunto de desarrollos, **TA** describe el hallazgo y analiza sus implicaciones para la actividad de la Autoridad (por ejemplo, la necesidad de actualizar políticas, posibles cambios en la demanda de certificación o ajustes en los procesos de supervisión). El borrador inicial deberá completarse durante el comienzo del nuevo año;

d) **Revisión y perfeccionamiento** — El **JAN** revisa en detalle el borrador del informe, verificando la exactitud y exhaustividad de la información y valorando la solidez del análisis y de las recomendaciones. El borrador podrá remitirse a otros responsables o expertos internos para que aporten comentarios sobre secciones específicas. El **JAN** formula observaciones y solicita aclaraciones o adiciones a **TA**. Este proceso iterativo de revisión se desarrolla durante varias semanas (habitualmente en enero y febrero), hasta que el informe alcanza el nivel requerido de calidad y exhaustividad;

e) **Aprobación y finalización** — Una vez incorporadas todas las revisiones, el **JAN** otorga la aprobación formal al informe interno. Se informará al Subdirector General del CCN (**SGCCN**) de la finalización del informe, proporcionándole una copia a efectos de conocimiento estratégico. El informe interno final se archivará en el Sistema de Información de la Autoridad Nacional de Certificación de la Ciberseguridad **(SGA)** para su conservación y futuras referencias.

4. FINALIZACIÓN Y DISTRIBUCIÓN

4. Tras la aprobación interna, se preparará una versión pública del informe de seguimiento para su difusión externa. Bajo la dirección del **JAN**, **TA** suprimirán cualquier información confidencial o de carácter deliberativo interno del informe aprobado, garantizando que el documento externo se centre en los desarrollos fácticos y en las observaciones generales. Se informará al **SED** de la versión depurada, que se comparte con las partes externas pertinentes. En particular, la **ANCC** transmite el informe público a **ENISA** y a los miembros del **GECC** (por ejemplo, a través del representante nacional en el **GECC** o mediante un canal seguro oficial), de conformidad con el artículo 62, apartado 4, letra f), del **[CSA]**, con el fin de facilitar el intercambio de información y de buenas prácticas.

5. El informe público también podrá ponerse a disposición en el sitio web de la Autoridad Nacional de Certificación de la Ciberseguridad **(WANCC)** con fines de transparencia, cuando se considere apropiado. Cuando sea posible, se solicitará confirmación de recepción a los destinatarios externos y se conservarán copias de la versión pública en el **SGA** junto con el informe interno. De este modo, la Autoridad contribuye a la toma de conciencia conjunta y a los esfuerzos de armonización entre los Estados miembros, asegurando que los resultados relativos a los desarrollos en la certificación de la ciberseguridad se compartan y examinen a escala europea.

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
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