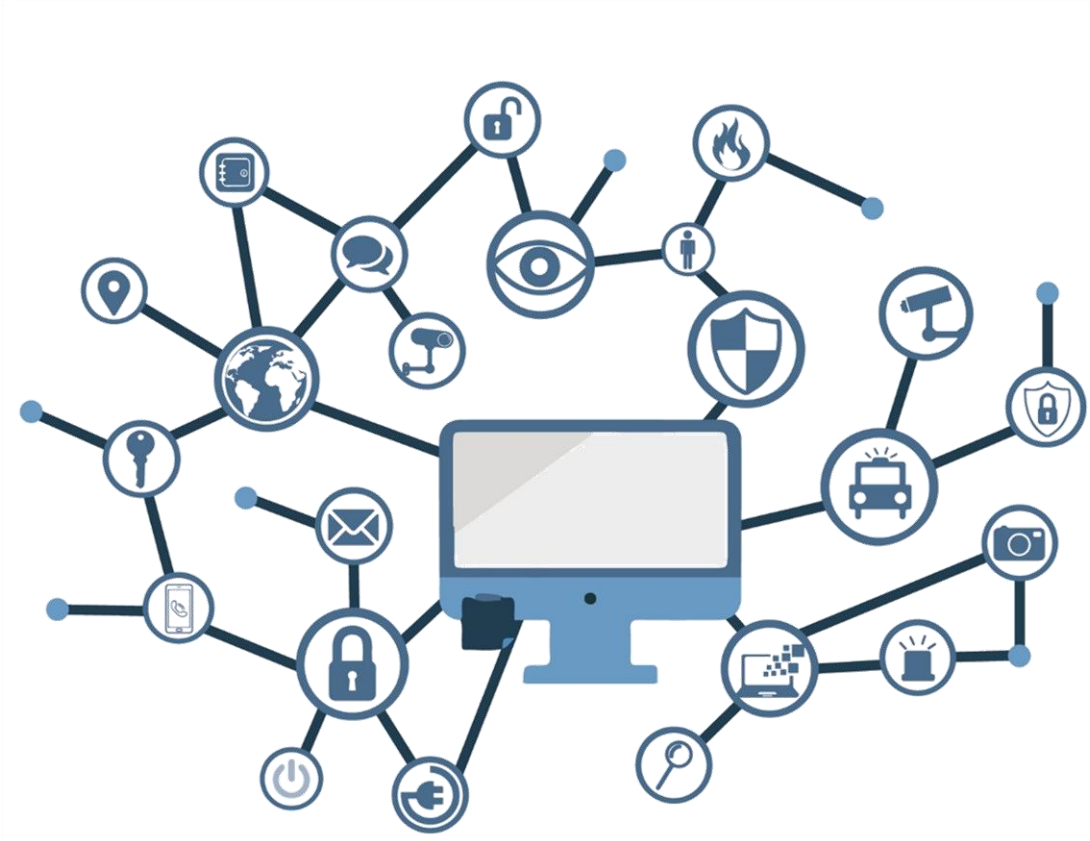
Autoridad Nacional de Certificación de la Ciberseguridad

centro criptológico nacional

ANCC-PO-07

Supervisión de cumplimiento



Marzo de 2026
Versión 1

MINISTERIO DE DEFENSA

CONTROL DE VERSIONES

Versión	Comentarios
1.0	Versión inicial

ÍNDICE

1. INTRODUCCIÓN

1. El presente procedimiento define la forma en que la Autoridad Nacional de Certificación **(ANCC)** supervisa y garantiza el cumplimiento, por parte de los productos y servicios **TIC** certificados, de sus procesos **TIC**, de los titulares de certificados **del esquema europeo de certificación de la ciberseguridad basado en los criterios comunes (EUCC)** y de los Organismos de Evaluación de Conformidad **(OEC)**, incluidos los **OC** y los **ITSEF**, de los requisitos establecidos en los esquemas europeos de certificación de la ciberseguridad. Abarca los mecanismos de supervisión continua, las auditorías e investigaciones, el muestreo de certificados, la tramitación de reclamaciones y las actuaciones que se adoptan en los casos de no conformidad o incumplimiento, según lo dispuesto en el **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 en el esquema **EUCC.**

2. ACTIVIDADES DE SUPERVISIÓN

2. La **ANCC** adopta un enfoque continuo y basado en el riesgo para la supervisión del cumplimiento de todos los certificados europeos de ciberseguridad emitidos. Este enfoque abarca la supervisión de los productos y servicios **TIC** certificados, de sus procesos **TIC**, de los titulares de certificados **EUCC** y de las actividades de los **OEC** autorizados (incluidos cada **OC** y los **ITSEF** asociados). El jefe de la unidad de la **ANCC (JAN)** dirigirá las tareas de supervisión. El personal técnico de la **ANCC (TA),** previamente asignado, se encargará de las tareas de supervisión específicas de cada esquema y prestará apoyo en la recopilación y el análisis de la información. Las siguientes fuentes y actividades principales alimentan la supervisión realizada por la **ANCC**:

a) **Intercambio de información**. Los flujos regulares de información procedentes de organizaciones relevantes respaldan la supervisión. La **ANCC** recopila aportaciones de los **OC** (por ejemplo, informes periódicos o notificaciones), de la Entidad Nacional de Certificación (**ENAC)** (en relación con el estado de acreditación o incidencias) y de otras autoridades de vigilancia del mercado u organismos europeos (como **ENISA** o el **GECC**), a fin de mantenerse informada sobre factores que puedan afectar al cumplimiento.

b) **Auditorías e inspecciones**. La **ANCC** realiza auditorías de los **OEC** y, cuando es necesario, inspecciones relacionadas con certificados concretos. Estas auditorías pueden programarse periódicamente o iniciarse a partir de indicadores de riesgo. Verifican que las actividades de certificación y los productos certificados continúan cumpliendo los requisitos aplicables. El **TA** prepara y ejecuta las auditorías, tanto *in situ* como a distancia.

c) **Muestreo**. La **ANCC** lleva a cabo comprobaciones proactivas sobre una muestra de certificados emitidos cada año (descrita en el programa de muestreo que se recoge más adelante). Este muestreo basado en el riesgo de productos **TIC** certificados ayuda a identificar de manera sistemática posibles no conformidades no detectadas.

d) **Reclamaciones e informes de incidentes**. La **ANCC** tiene en cuenta las reclamaciones, los informes de vulnerabilidades u otra información sobre incidentes procedente de titulares de certificados, usuarios, investigadores de seguridad u otras partes interesadas. Dichos recursos se registran y analizan como posibles indicadores de incumplimiento y pueden dar lugar a investigaciones adicionales cuando proceda (véase el «*ANCC-PO-05, Gestión de reclamaciones*»).

e) **Seguimiento de amenazas**. La **ANCC** realiza un seguimiento de la evolución del panorama de amenazas en ciberseguridad para garantizar que el nivel de garantía proporcionado por los certificados existentes siga siendo válido. Se rastrean las amenazas emergentes, las vulnerabilidades y los cambios tecnológicos que puedan menoscabar las garantías de seguridad certificadas. Cuando proceda, la **ANCC** evalúa si los productos certificados requieren una

reevaluación o medidas adicionales (en coordinación con el **OC** emisor), de conformidad con los procedimientos de gestión de vulnerabilidades.

3. AUDITORÍAS E INVESTIGACIONES

3. La **ANCC** realiza auditorías e investigaciones de cumplimiento para verificar, cuando resulte necesario, la observancia de los requisitos de certificación por parte de los **OEC**. Estas actuaciones pueden iniciarse como parte del programa de supervisión planificada o activarse por preocupaciones específicas (por ejemplo, indicios de posible no conformidad, reclamaciones o resultados del programa de muestreo). Las auditorías pueden incluir revisiones documentales, evaluaciones in situ o a distancia y, en determinados casos, visitas a las instalaciones de los titulares de certificados, haciendo uso de la facultad de acceso a las instalaciones de la autoridad de conformidad con los procedimientos legales aplicables. Todas las investigaciones se llevan a cabo respetando el Derecho de la Unión y el Derecho nacional, incluidos los requisitos del procedimiento administrativo establecidos en **Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas [LPAC]**.

4. Normalmente, el **TA** ejecuta las tareas rutinarias de auditoría y de obtención de hechos. El **JAN** aprueba la apertura de toda investigación significativa o auditoría extraordinaria, mientras se mantiene informado de los principales expedientes de cumplimiento en curso. Cuando sea necesario, la **ANCC** podrá implicar a expertos externos o cooperar con **ENAC** (por ejemplo, mediante evaluaciones conjuntas con los evaluadores de acreditación) para reforzar la eficacia de la investigación.

5. Cuando una investigación afecte a un producto **TIC** certificado concreto o a su titular, la **ANCC** informará al titular del certificado, al **OC** correspondiente y, en su caso, al **ITSEF** implicado de que dicha investigación está en curso. Esta comunicación garantiza la transparencia y facilita la colaboración de estas entidades. Si la investigación tiene implicaciones transfronterizas (por ejemplo, cuando se trate de un producto certificado por un **OC** en otro Estado miembro), la **ANCC** se coordinará con la otra autoridad nacional de certificación de la ciberseguridad para cooperar en la investigación o compartir sus resultados.

6. Todas las no conformidades identificadas durante auditorías, inspecciones o investigaciones de incidentes serán gestionadas de manera sistemática por la **ANCC**. El proceso comprenderá:

    a) **Registro:** El **TA** registrará cada no conformidad en el **SGA**, incluyendo descripción, gravedad y fecha de identificación.

    b) **Notificación:** El **JAN** (o el **TA** en su nombre) notificará formalmente la no conformidad al **OEC**, indicando las medidas correctoras exigidas y el plazo para su resolución.

    c) **Corrección y verificación:** El **OEC** implementará las medidas correctoras. El **TA** supervisará el progreso y verificará que la no conformidad haya sido resuelta de manera eficaz (incluyendo, si procede, una revisión o inspección de seguimiento).

d) **Cierre y escalado:** El **JAN** revisará la resolución. Si está conforme, cerrará formalmente la no conformidad en el Sistema de Información de la Autoridad Nacional de Certificación de la Ciberseguridad **(SGA)**. Si no se corrige dentro del plazo o es recurrente, el **JAN** escalará el asunto, pudiendo emitir advertencias, imponer restricciones operativas o recomendar iniciar la suspensión o retirada de la autorización del **OEC**, de conformidad con los requisitos del procedimiento administrativo aplicable.

4. MUESTREO DE CERTIFICADOS

7. La **ANCC** aplica un programa anual de muestreo para evaluar de forma proactiva el cumplimiento continuo de los productos certificados. Cada año, al menos el **4%** de todos los certificados **EUCC** válidos se selecciona para una revisión, según lo exigido por el esquema. La selección de esta muestra es coordinada por el **TA** y se basa en una evaluación de riesgos realizada en cooperación con otras autoridades de vigilancia del mercado pertinentes. Este enfoque garantiza que el muestreo se centre en los certificados con mayor probabilidad de aportar conclusiones significativas (por ejemplo, los asociados a perfiles de riesgo elevados).

8. La ANCC puede establecer un nivel de muestreo de seguimiento en dos niveles, en base a:

   - **Seguimiento:** Revisión limitada a la documentación emitida por el OC, con el fin de verificar la consistencia documental, la conformidad con los requisitos formales del esquema y la ausencia de señales de alerta iniciales.
   - **Revisión:** Revisión exhaustiva que incluye tanto la parte de certificación como la parte de evaluación (documentación técnica, evidencias, informes del ITSEF, actividades de ensayo, trazabilidad de requisitos, análisis de vulnerabilidades, etc.). Este tipo de muestreo podrá reutilizar las actividades previstas en el procedimiento «*ANCC-PO-06 Procedimiento de autorización y supervisión para el uso de la marca CCRA en el esquema EUCC*».

9. Para elegir la muestra de productos **TIC** certificados que se revisarán se utilizan criterios objetivos. Entre los factores considerados se incluyen la categoría de producto, el nivel de garantía, los titulares concretos de certificados, el **OC** emisor y cualquier **ITSEF** implicado, así como otra información disponible para la **ANCC** (como problemas de seguridad conocidos o información proporcionada por autoridades de vigilancia del mercado). El **TA** documenta en el **SGA** la justificación y los factores de riesgo relativos a cada selección.

10. Una vez determinada la muestra anual, la **ANCC** notifica la selección a los titulares de los certificados afectados. Para cada producto **TIC** seleccionado se comunica a su titular del certificado **EUCC** la razón de la selección.

11. Para cada certificado **EUCC**, el **TA** asignado, confirmará que el certificado y su informe de certificación se ajustan al formato prescrito e incluyen todos los elementos necesarios marcados por **[EUCC]** (p. ej. nombre y versión del producto evaluado, nivel de garantía, periodo de validez, referencias a Perfiles de Protección o normas aplicadas, organismo de certificación y, en su caso, la instalación de la configuración evaluada) y que el **OC** emisor está acreditado por el **ENAC** y debidamente autorizado o notificado para el esquema **EUCC**. En el caso de una autoevaluación de conformidad **UE** al amparo del **CSA**, TA comprobará que la declaración **UE** de conformidad esté debidamente firmada por la parte responsable y que la documentación técnica adjunta sea suficiente para respaldar la declaración de conformidad.

12. La **ANCC** analiza los resultados de cada revisión derivada del muestreo, a fin de determinar si existe alguna no conformidad, deficiencia procedimental o debilidad de seguridad. Si se considera que un producto muestreado puede no cumplir los requisitos, el caso se puede elevar a una investigación completa u otras medidas apropiadas conforme al presente procedimiento (por ejemplo, solicitud de información adicional mediante requerimiento al **OC** o al **ITSEF**).

13. Todas las actividades de muestreo y sus resultados se registran debidamente en el SGA, lo que proporciona el registro sobre la evaluación de riesgos, los criterios de selección, el nivel de muestreo aplicado y los resultados obtenidos asociados a la supervisión.

14. Las conclusiones extraídas del programa de muestreo se integran en la mejora de la estrategia global de supervisión y pueden dar lugar a ajustes en los criterios de riesgo, en la frecuencia de muestreo o en la orientación proporcionada a los organismos de certificación.

5. GESTIÓN DE RECLAMACIONES RELACIONADAS CON EL CUMPLIMIENTO

15. La **ANCC** mantiene canales (por ejemplo, a través del sitio web de la autoridad (**WANCC**) o de puntos de contacto designados) para que cualquier parte pueda presentar reclamaciones o informes relativos a presunto incumplimiento. Tales reclamaciones pueden referirse a problemas con productos **TIC** certificados, a titulares de certificados o a la actuación de **OEC**. Tras la recepción de una reclamación, el **TA** la registra en el **SGA** y realiza una revisión inicial para evaluar su credibilidad y relevancia.

16. Si la reclamación aporta indicios verosímiles de incumplimiento, la **ANCC** inicia las actuaciones de seguimiento oportunas. Estas pueden incluir la solicitud de información adicional a las partes concernidas (el **OC** correspondiente, la **ITSEF** implicada o el titular del certificado), así como la apertura de una investigación o de una auditoría ad hoc centrada en las cuestiones planteadas. En algunos casos, el objeto de la reclamación puede incluirse en el siguiente ciclo de muestreo para un examen más detallado. A lo largo del proceso, el reclamante es informado, en la medida de lo posible, sobre el estado y el resultado de su reclamación. La tramitación de las reclamaciones se ajusta a los principios y plazos del procedimiento aplicable (véase el «*ANCC-PO-05 Gestión de reclamaciones*»).

6. ACTUACIONES ANTE EL INCUMPLIMIENTO

17. Cuando mediante las actividades de supervisión descritas anteriormente se identifican no conformidades o infracciones, la **ANCC** adopta las medidas apropiadas para abordarlas y hacer cumplir las obligaciones de certificación. La respuesta se adapta a la naturaleza del problema (ya se refiera a un producto **TIC** certificado, a un titular de certificado o a un **OEC**) y a la gravedad de su impacto sobre la ciberseguridad. Todas las actuaciones de ejecución se llevan a cabo de conformidad con los requisitos legales nacionales en materia de procedimiento administrativo (por ejemplo, las garantías y etapas previstas en **[LPAC]**), lo que incluye ofrecer a las entidades afectadas la oportunidad de ser oídas y de corregir las deficiencias, cuando sea posible, antes de que se adopte una decisión final.

18. Si se constata que un producto **TIC** certificado no se ajusta a los requisitos de su certificado **EUCC** o del esquema, la **ANCC**, en coordinación con el **OC** emisor, se asegurará de que se adoptan medidas correctoras. El titular del certificado podrá recibir instrucciones (a través del organismo de certificación) para remediar las vulnerabilidades o no conformidades identificadas dentro de un plazo determinado. Se espera que el organismo de certificación suspenda el certificado si el problema es grave o no se remedia con prontitud. En casos de no conformidad grave, o cuando fracasen los intentos de subsanación, el certificado se retirará. De conformidad con el **[CSA],** la **ANCC** está facultada para retirar por sí misma un certificado europeo de ciberseguridad —incluidos los emitidos por un **OC**— con el fin de proteger de manera rápida al público, cuando sea necesario.

19. Para los certificados que se suspendan como consecuencia de problemas detectados, el **JAN** podrá autorizar prórrogas del período de suspensión (que no excederán de un año en total) en circunstancias debidamente justificadas, a fin de conceder al titular tiempo adicional para aplicar las medidas correctoras. Si, transcurrido dicho plazo, el problema no se ha resuelto adecuadamente, la suspensión se convertirá en retirada definitiva del certificado, salvo que existan motivos legales imperiosos para decidir lo contrario.

20. Cuando un titular de certificado incumpla las obligaciones que le impone el esquema (por ejemplo, no aplicar las actualizaciones de seguridad requeridas o utilizar indebidamente el certificado en su comunicación comercial), la **ANCC** podrá ordenar al **OC** correspondiente que imponga condiciones adicionales, restrinja el alcance del certificado o lo suspenda o retire. El **TA** preparará una evaluación del caso, incluyendo las obligaciones incumplidas, el impacto potencial y las medidas correctoras propuestas, para su consideración por el **JAN**.

21. En los supuestos de incumplimiento por parte de un **OEC**, la **ANCC** evaluará si las deficiencias detectadas cuestionan la fiabilidad de las actividades de evaluación de la conformidad. Dependiendo de la gravedad, las medidas podrán incluir la imposición de acciones correctoras obligatorias, la suspensión o retirada de la autorización del **OEC** para operar en el marco de los esquemas europeos, así como la coordinación con **ENAC** para revisar la acreditación del organismo. La **ANCC** también valorará el impacto sobre

los certificados emitidos por dicho **OEC** y, en su caso, iniciará las acciones previstas en el presente procedimiento (suspensión, reevaluación o retirada de certificados).

22. Todas las decisiones significativas de ejecución —como la suspensión o retirada de certificados, o la suspensión o retirada de la autorización de un **OEC** — son adoptadas formalmente por los órganos directivos de la **ANCC**. El **JAN** examina las conclusiones del caso propuestas por el **TA** y elevará la decisión de actuación al Secretario de Estado Director del CCN **(SED)**, quien en su caso tras valoración podrá firmar dicha decisión. A lo largo del proceso de ejecución, el **TA** apoya la preparación de las resoluciones, la comunicación de las decisiones a las partes afectadas y la implantación de las medidas de seguimiento (por ejemplo, garantizar que los certificados retirados se eliminan de los listados públicos pertinentes).

7. COMUNICACIÓN Y CONSERVACIÓN DE LA INFORMACIÓN

23. La **ANCC** garantiza que los resultados de las actividades de supervisión del cumplimiento y de las actuaciones de ejecución se comunican a las partes pertinentes y que todas las etapas se documentan adecuadamente. Siempre que una investigación o una actuación de ejecución tenga implicaciones transfronterizas (por ejemplo, cuando afecte a un certificado emitido por un **OC** de otro Estado miembro o a productos disponibles en varios Estados miembros), la **ANCC** informará a las demás autoridades nacionales de certificación de la ciberseguridad afectadas. De conformidad con las obligaciones del esquema **EUCC**, la **ANCC** informará igualmente al Grupo Europeo de Certificación de la Ciberseguridad (**GECC)** sobre estos casos transfronterizos y los resultados de las investigaciones, facilitando así la cooperación y el intercambio de información a escala europea.

24. Cuando la no conformidad o el problema de seguridad detectado pueda ser relevante a efectos de otra normativa de la Unión (por ejemplo, legislación sectorial sobre productos), la **ANCC** notificará la información pertinente a las autoridades nacionales competentes, incluidas las autoridades de vigilancia del mercado, según proceda. La **ANCC** cooperará con dichas autoridades para garantizar que las medidas adoptadas sean coherentes y se coordinen adecuadamente, evitando duplicidades y lagunas en la protección.

25. Todas las actividades de supervisión del cumplimiento y sus resultados se documentan en el **SGA**. Ello incluye los informes de auditoría, las conclusiones de las investigaciones, las decisiones sobre el estado de los certificados o de la autorización de **OEC** y la correspondencia con las entidades implicadas. Las actuaciones clave (por ejemplo, la suspensión o retirada de un certificado, o la imposición de sanciones a un **OEC**) también se reflejan en el sitio web de la Autoridad Nacional de Certificación de la Ciberseguridad cuando proceda, actualizando los listados públicos de productos certificados o publicando avisos sobre cambios en la validez de los certificados. Estos registros y resultados garantizan la trazabilidad y la rendición de cuentas en cada caso, y se integran en las obligaciones periódicas de información de la **ANCC**. En particular, la información agregada sobre la supervisión del cumplimiento (como el número de auditorías realizadas, certificados retirados y otras estadísticas y observaciones relevantes) se incluye en el informe anual de resumen remitido a **ENISA** y al **GECC** (véase el «*ANCC-PO-01 Informe anual*»), contribuyendo así a la supervisión y mejora del marco europeo de certificación de la ciberseguridad.

8. 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)

9. 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