OC-CN

CCN
centro criptológico nacional

Procedimiento Operativo
PO-EUCC-13

Monitorización y control

Julio 2025
Versión 1.0

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.

AVISO LEGAL

ÍNDICE

1. Referencias

L21/92	Ley 21/1992, de 16 de julio, de Industria.
L39/15	Ley 39/15, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
L40/15	Ley 40/15, de 1 de octubre, de Régimen Jurídico del Sector Público.
L11/02	Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.
RD2200/95	RD 2200/1995, de 28 de diciembre, por el que se aprueba el Reglamento de la Infraestructura para la calidad y seguridad industrial.
RD436/02-RD612/06	Real Decreto 436/2002, de 10 de mayo, por el que se establece la estructura orgánica del Centro Nacional de Inteligencia, modificado por el Real Decreto 612/2006, de 19 de mayo.
RD593/02	Real Decreto 593/2002, de 28 de junio, por el que se desarrolla el régimen económico presupuestario del Centro Nacional de Inteligencia, modificado por el Real Decreto 1287/2005, de 28 de octubre.
RD327/04	Real Decreto 327/2004, de 27 de febrero, por el que se modifica el Estatuto del personal del Centro Nacional de Inteligencia, aprobado por el Real Decreto 1324/1995, de 28 de julio.
RD421/04	Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional.
RD462/02	Real Decreto 462/2002, de 24 de mayo, sobre indemnizaciones por razón del servicio.
ISO17065	UNE-EN ISO/IEC 17065, Evaluación de la conformidad. Requisitos para organismos que certifican productos, procesos y servicios.
SGOC	Sistema de Gestión del OC/ANCC.
OC/ANCC	Organismo de Certificación de la Autoridad Nacional de Certificación de la Ciberseguridad
CB	*Certification Body* (OC/ANCC)

ETR	*Evaluation Technical Report* (Informe Técnico de Evaluación)
CSA	Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
EUCC	Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC) Commission Implementing Regulation (EU) 2024/3144 of 18 December 2024 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation
SOTA	State-of-the-art documents in their applicable version at the date of execution of this procedure; 'Accreditation of ITSEFs for the EUCC'; 'Accreditation of CBs for the EUCC'

2. Normativa interna del OC/ANCC

La normativa interna del Organismo de Certificación de la Autoridad Nacional de Certificación de la Ciberseguridad (OC/ANCC) se puede ver en el documento LIS-EUCC-08.

3. Objeto

Establecer las fases, actividades y responsabilidades para la monitorización continua de:

- Los certificados de ciberseguridad emitidos por el OC/ANCC bajo el esquema EUCC.
- Los laboratorios ITSEFs autorizados para realizar evaluaciones conforme al Reglamento (UE) 2019/881 y el Reglamento de Ejecución (UE) 2024/482 que realizan actividadades de evaluación para el OC/ANCC.

4. Ámbito de aplicación

Este procedimiento aplica a:

- Todos los certificados EUCC emitidos por el OC/ANCC.

- Todos los laboratorios ITSEFs cualificados por el OC/ANCC para realizar evaluaciones EUCC.
- Personal técnico y administrativo del organismo de certificación.

5. Monitorización de Certificados EUCC Emitidos

Esta fase tiene como objetivo verificar la vigencia, conformidad y seguridad de los productos TIC certificados bajo el esquema EUCC. El organismo de certificación debe realizar actividades periódicas y reactivas para asegurar que los certificados emitidos siguen cumpliendo los requisitos establecidos.

5.1 Registro de certificados

El OC/ANCC mantendrá una base de una base de datos actualizada con: ID, producto, fabricante, nivel de garantía, fecha de emisión, validez, estado para cada certificado EUCC emitido. Esta base de datos conforma el LIS-EUCC-01.

5.2 Revisión de vigencia

El ***Responsable de calidad realizará*** las siguientes acciones*:*

- ***Verificar*** la relación de productos certificados cuya fecha de expiración se enmarca en los próximos 6 meses y ***notificar*** al solicitante de tal hecho por si desea comenzar un proceso de continuidad de la garantía del certificado.
- ***Verificar*** continuamente que los certificados emitidos no hayan expirado y ***notificará*** con al menos una semana de antelación al solicitante y a ENISA de la fecha de expiración del certificado para su retirada.
- **Verificar** trimestralmente que la lista de productos certificados de ENISA es mantenida correctamente verificando que los certificados publicados no hayan expirado, hayan sido revocados o suspendidos. En caso de detectar alguna desviación, ***informar*** inmediatamente a ENISA de las desviaciones detectadas.

5.3 Auditoría documental de cumplimiento

Anualmente, el ***Responsable de calidad realizará*** las siguientes acciones*:*

- Realizará un muestro de los certificados emitidos seleccionando al menos una muestra correspondiente al 4% de los certificados emitidos, registrando el certificado y documentación asociada al mismo.
- Notificará al ***Certificador*** responsable de procedimiento el inicio de una auditoría documental de cumplimiento.

El ***Certificador*** responsable del expediente de certificación ***realizará*** las siguientes acciones:

- Comprobará que la información de ciberseguridad relativa al producto certificado sigue siendo vigente y se corresponde a las versiones evaluadas en el procedimiento de certificación.
- Muestreará en las bases de datos de vulnerabilidades potenciales vulnerabilidades del TOE certificado.
- Comprobará que la información del certificado publicada sigue siendo vigente.
- Elevará un *Informe de cumplimiento* al Responsable de calidad, indicando la vigencia del cumplimiento del expediente.

El ***Responsable de calidad realizará*** las siguientes acciones*:*

- Si el cumplimiento sigue vigente, aprobará y registrará el informe.
- Si existen desviaciones en el cumplimiento, generará una Notificación de desviación de cumplimiento que será revisada por el Responsable Técnico y aprobada por el Jefe de Área de Certificación en la que se informará al solicitante de dichas desviaciones y los plazos para solventarlas de la siguiente manera:
    - Las relativas a la información de ciberseguridad o uso de producto certificado se proporcionará un plazo de 15 días naturales al solicitante para solventarlas. En caso de no solventarse en dicho plazo o no recibir respuesta con las acciones correctivas, se notificará a la ANCC y se iniciará procedimiento de suspensión del certificado en la lista de productos certificados. Si pasados 3 meses de la suspensión del certificado no se han corregido las deficiencias se iniciará el procedimiento de retirada del certificado.
    - Las relativas a vulnerabilidades al producto certificado se notificará al solicitante dicho punto y se seguirá lo indicado por el procedimiento PO-EUCC-014.

5.4 Seguimiento de incidentes

Semestralmente, el *Responsable Técnico* ***realizará*** las siguientes acciones*:*

- Realizará un muestro de los certificados emitidos seleccionando al menos una muestra correspondiente al 4% de los certificados emitidos, registrando el certificado y documentación asociada al mismo.
- Notificará al ***Certificador*** responsable de procedimiento el inicio de una auditoría documental de cumplimiento.

El ***Certificador*** responsable del expediente de certificación ***realizará*** las siguientes acciones:

- Muestreará en las bases de datos de vulnerabilidades potenciales vulnerabilidades del TOE certificado.
- Elevará un *Informe de cumplimiento* al Responsable Técnico, indicando la existencia de vulnerabilidades públicas que afecten al producto certificado.

El ***Responsable Técnico realizará*** las siguientes acciones*:*

- Si el cumplimiento sigue vigente, aprobará y registrará el informe.

- Adicionalmente, si existen a vulnerabilidades en el producto certificado se notificará al solicitante dicho punto y se seguirá lo indicado por el procedimiento PO-EUCC-014.

6. Monitorización de Laboratorios ITSEFs

Esta fase tiene como objetivo asegurar que los laboratorios ITSEFs autorizados mantienen su competencia técnica, acreditación y conformidad con los requisitos del esquema EUCC. El organismo de certificación debe supervisar su desempeño y realizar auditorías periódicas.

6.1 Verificación de acreditación

El *Responsable de Calidad* ***registrará*** en el listado EUCC-LIS-02 las fechas de expiración de la acreditación y autorización de los laboratorios cualificados.

El *Responsable de Calidad* ***confirmará*** ante la notificación del laboratorio cualificado o trimestralmente que el laboratorio mantiene su acreditación ISO/IEC 17025 y autorización nacional vigente. En caso de aproximarse la fecha de expiración, notificará al laboratorio de la necesidad de actualizar la información del estado de la autorización y acreditación, requiriendo la actualización de la acreditación y autorización antes de su expiración.

6.2 Revisión de desempeño técnico

Los ***Certificadores*** responsables de expedientes de certificación evaluarán semestralmente la calidad de los informes de evaluación, tiempos de entrega y cumplimiento técnico y elevarán un Informe de desempeño técnico al Responsable de Técnico quien incorporará de manera general las apreciaciones de los informes en el orden del día de la Reunión de consistencia Técnica conforme al procedimiento PO-EUCC-07.

El ***Responsable Técnico*** en caso de que detecte que las desviaciones técnicas de las actividades de evaluación del laboratorio puedan poner en riesgo la actividad de certificación, notificará al laboratorio de las desviaciones detectadas de la siguiente manera:

- Reiteración de desviaciones menores: elevará informe justificado y proporcionará un plazo de 3 meses al laboratorio para proporcionar un plan de acciones correctivas. En caso de no recibirse respuesta o que el plan de acciones correctivas no solvente las deficiencias se notificará al laboratorio y a la ANCC de la suspensión temporal de la cualificación proporcionando un plazo de 3 meses para alegaciones adicionales antes de la retirada de la cualificación del laboratorio.

- Desviaciones críticas: se notificará al laboratorio y a la ANCC de la suspensión temporal de la cualificación proporcionando un plazo de 3 meses para alegaciones adicionales para solventar las desviaciones antes de la retirada de la cualificación del laboratorio.

7. Evaluación de Desempeño y Mejora Continua

Esta fase tiene como objetivo medir la eficacia del sistema de monitorización y control, y proponer mejoras continuas en los procesos del organismo de certificación. Se basa en indicadores clave de desempeño (KPIs) y en la revisión periódica del procedimiento.

7.1 Cálculo de KPIs

El *Responsable de Calidad* para verificar propondrá antes de un año de la entrada en vigor del procedimiento la propuesta de indicadores clave de desempeño (KPIs) (ej. porcentaje de certificados revisados, número de incidentes detectados, tiempos de respuesta y satisfacción de partes interesadas) para evaluar el desempeño de la monitorización y controlo del OC/ANCC.

7.2 Publicación de informes

El *Responsable de Calidad* anualmente elaborará un Informe de desempeño del procedimiento de monitorización y control en base a los indicadores claves de desempeño.

7.3 Revisión anual del procedimiento

El *Responsable de Calidad,* en base al desempeño medido, ***actualizará*** el procedimiento conforme a cambios normativos, tecnológicos o de experiencia operativa.

7.4 Reuniones de coordinación

El OC/ANCC estará informado y participará en reuniones con la ANCC, ENISA y otros organismos europeos para compartir buenas prácticas y coordinar acciones en relación a los procedimientos de monitorización y control del procedimiento.