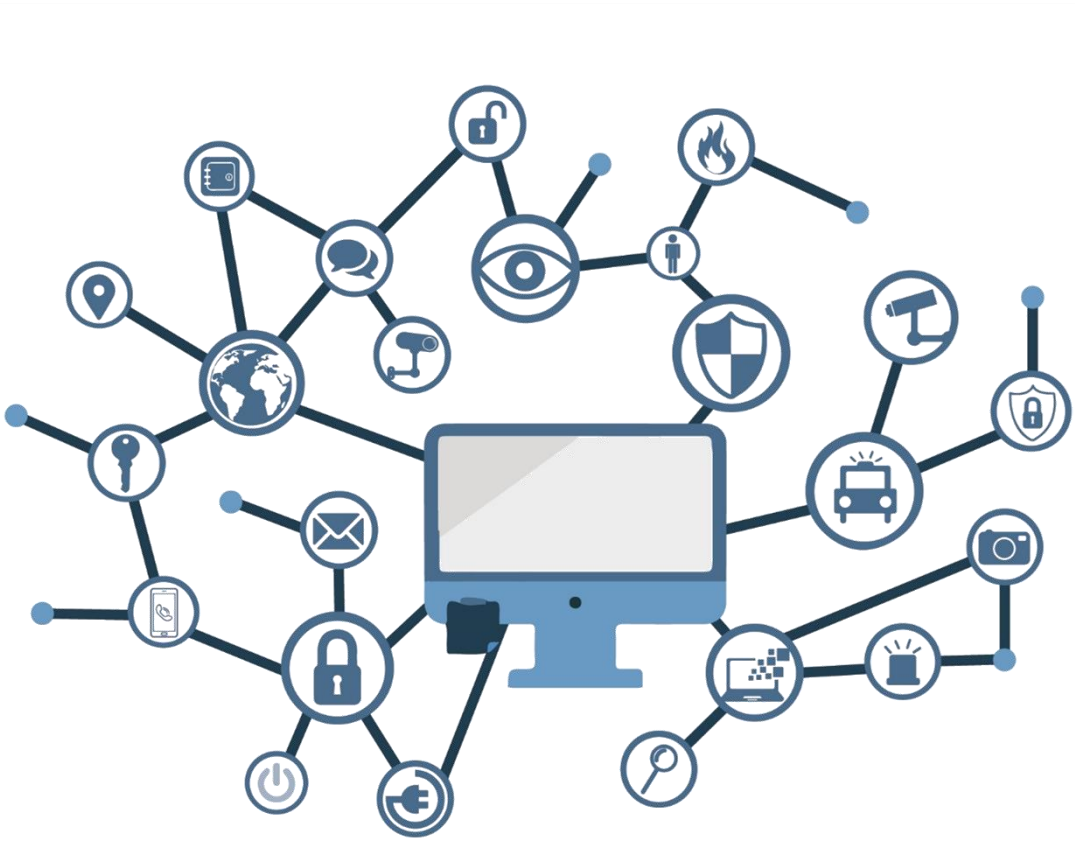
OC-CN

CCN
centro criptológico nacional

Procedimiento Operativo
PO-EUCC-14

Vulnerability Handling



Marzo 2025
Versión 1

MINISTERIO DE DEFENSA

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'
ENISA	Guidance on EUCC certificate lifecycle
ISO/IEC 30111	Vulnerability handling processes
ISO/IEC 29147	Vulnerability disclosure

2. Normativa interna del Organismo de Certificación

La normativa interna del OC se puede ver en el documento LIS-EUCC-008.

3. Objeto

Establecer el procedimiento de gestión de vulnerabilidades aplicable a los productos certificados bajo el esquema EUCC, garantizando la continuidad del cumplimiento con los requisitos de seguridad durante el ciclo de vida del certificado.

4. Alcance

Este procedimiento aplica a todos los certificados activos emitidos por el OC/ANCC.

5. Responsabilidades

- **Titular del Certificado:** Debe informar cualquier vulnerabilidad identificada que afecte a su producto certificado y aplicar las medidas correctivas oportunas.
- **OC/ANCC:** Recibe, evalúa y gestiona la información sobre vulnerabilidades. Puede requerir acciones al titular del certificado.
- **Responsable Técnico:** Coordina el proceso de gestión de vulnerabilidades.
- **Certificador designado:** Apoya en el análisis técnico de las vulnerabilidades cuando se requiera.

6. Flujo de Gestión de Vulnerabilidades

6.1 Notificación de Vulnerabilidad

- Cualquier parte interesada (titular, usuario, ITSEF, OCEUCC, CERT, ENISA, investigadores, etc.) puede notificar una vulnerabilidad al OC/ANCC mediante correo electrónico seguro o canal habilitado.
- El OC/ANCC registrará todas las notificaciones en un registro interno con identificador único.

6.2 Clasificación Inicial

- Se realiza una evaluación inicial para clasificar la vulnerabilidad:
    - **Crítica:** Afecta al cumplimiento de los requisitos esenciales del EUCC.
    - **Media:** Puede mitigarse sin invalidar los requisitos.
    - **Menor:** No afecta directamente al cumplimiento, pero puede afectar a la percepción del producto.

6.3 Evaluación de Impacto

- El CB analiza el impacto de la vulnerabilidad sobre los requisitos del certificado, con apoyo del evaluador si es necesario.
- Se decide si:
    - La vulnerabilidad invalida total/parcialmente el certificado.
    - Requiere medidas mitigadoras por parte del fabricante.
    - No tiene impacto relevante.

6.4 Comunicación al Titular

- En caso de que el descubrimiento no provenga del propio titular, el CB informará formalmente al mismo.
- Se solicitará:
  - Análisis de causa raíz.
  - Plan de acciones correctivas.
  - Cronograma de aplicación del parche o actualización.
  - Comunicación a usuarios finales si aplica.

6.5 Seguimiento y verificación

- El CB revisará el plan propuesto y podrá requerir evidencia adicional.
- El plan debe ejecutarse en un plazo máximo de 90 días (o plazo acordado según el impacto).
- El CB podrá requerir una reevaluación parcial del producto.

6.6 Resultados y decisiones

- Si las medidas son adecuadas:
  - El certificado se mantiene activo.
  - Se documenta la resolución en el expediente.
- Si las medidas no se aplican en plazo:
  - El CB podrá suspender temporalmente el certificado.
  - Si no se corrige, se procede a la revocación.

6.7 Comunicación a ENISA

- Si la vulnerabilidad tiene impacto significativo, el CB notificará a ENISA conforme a los mecanismos establecidos.
- ENISA podrá coordinar acciones o emitir directrices adicionales.

7. Revisión del Procedimiento

El procedimiento se revisará anualmente o tras la publicación de nuevas directrices por parte de ENISA.

8. ANEXO I Formulario de Reporte de Vulnerabilidad

Código: FORM-EUCC-VULN-01
Versión: 1.0

1. Información General

- **Nombre del producto certificado:**
  [Nombre comercial y versión del producto afectado]
- **Número de certificado EUCC:**
  [Identificador completo del certificado emitido]
- **Titular del certificado:**
  [Nombre de la organización titular]
- **Persona de contacto técnico:**
  - Nombre: _____
  - Cargo: _____
  - Correo electrónico: _____
  - Teléfono (opcional): _____

2. Detalles de la Vulnerabilidad

- **Identificador público (si aplica):**
  [Ej. CVE-2025-XXXXX, referencia de CERT, etc.]
- **Descripción técnica de la vulnerabilidad:**
  [Explicación clara y concisa de la vulnerabilidad]
- **Origen del descubrimiento:**
  ☐ Descubrimiento interno
  ☐ Reportado por terceros
  ☐ Informado por el CB
  ☐ Otro: _____
- **Condiciones de explotación:**
  [Ej. acceso físico, red local, remoto, etc.]
- **Impacto sobre el producto certificado:**
  [Indicar el posible incumplimiento de requisitos de seguridad del EUCC, afectación de activos, etc.]

- **¿Está la vulnerabilidad ya explotada o hay evidencia de explotación activa?**
  ☐ Sí
  ☐ No
  ☐ No se puede determinar

3. Análisis de Causa Raíz

- **Análisis técnico de la causa:**
  [Describir el origen del fallo: error de diseño, configuración, implementación, etc.]
- **¿La vulnerabilidad afecta otras versiones o variantes del producto?**
  ☐ Sí
  ☐ No
  ☐ No se ha evaluado
  [Detalles si aplica]

4. Plan de Acción Correctiva

- **Medida(s) correctiva(s) previstas:**
  [Parche, actualización, configuración, retirada del producto, etc.]
- **Fecha estimada de disponibilidad de la solución:**
  [dd/mm/aaaa]
- **Método de distribución de la solución:**
  [Por ejemplo: actualización automática, instalación manual, asistencia técnica, etc.]
- **¿Requiere validación o reevaluación por parte del CB?**
  ☐ Sí
  ☐ No
  [Justificar si aplica]

5. Comunicación a Usuarios Finales

- **¿Está previsto notificar a los usuarios afectados?**
  ☐ Sí
  ☐ No
  [Adjuntar comunicado si aplica]
- **Medios previstos para la comunicación:**
  ☐ Web corporativa
  ☐ Boletín de seguridad

☐ Correo a clientes

☐ Otro: _____

6. Documentación Adjunta

☐ Evidencias técnicas (p. ej. pruebas de concepto, informes de terceros)

☐ Cronograma detallado de resolución

☐ Copia del comunicado al cliente

☐ Otro: _____

7. Declaración del Titular

Por la presente, declaro que la información proporcionada en este formulario es veraz y completa, y autorizo al Certification Body a utilizarla en el marco de sus funciones de supervisión bajo el esquema EUCC.

- **Nombre y firma:**
- **Fecha:**
- **Sello de la organización (si aplica):**