centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 2003

Plantilla para la Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad (LINCE)

Marzo 2022

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.03.22 11:38:17 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-090-9

Fecha de Edición: Marzo 2022.

CONTROL DE VERSIÓN

Versión	Comentario	Fecha
0.1	Versión en pruebas	Junio 2018
1.1	MEB	Octubre 2021
1.2	Errata	Noviembre 2021
2.0	Actualización MEB	Marzo 2022

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

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Marzo de 2022

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

1. Este documento es una plantilla de referencia para redactar la Declaración de Seguridad del producto para la Certificación Nacional Esencial de Seguridad.

1.1 INFORMACIÓN DEL PATROCINADOR, TOE Y EVALUACIÓN

Datos del Solicitante (Nombre y Dirección)	
Datos del Desarrollador (Nombre y Dirección)	
Nombre del TOE	
Versión del TOE	
Taxonomía del producto según CCN-STIC-140 y su versión	Ej.- Anexo F.11: Herramientas de videoidentificación, versión 2.0. o NO APLICA [1] [2]
Tipo de evaluación (incluir los módulos opcionales)	Ej.- LINCE + MEC + MCF + MEB
Manuales de uso del producto y su versión	

1.2 METODOLOGÍA Y CRITERIOS DE EVALUACIÓN

CCN-STIC-2001	CCN-STIC-2001 - Definición de la Certificación Nacional Esencial de Seguridad, versión 2.0. Marzo 2022.
CCN-STIC-2002	CCN-STIC-2002 - Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad, versión 2.0. Marzo 2022.
…	….

[1] En caso de que la declaración de seguridad no cumpla estrictamente con todos los requisitos marcados en los anexos definidos por los responsables del CPSTIC en la CCN-STIC-140.
[2] La declaración de seguridad deberá ser aprobada por parte de los responsables del CPSTIC.

2. DESCRIPCIÓN DEL TOE

2.1 DESCRIPCIÓN FUNCIONAL DEL TOE

2. Una descripción del TOE incluyendo en lenguaje natural sus componentes principales y las principales funciones de seguridad que son objeto de la evaluación y certificación.

2.2 IDENTIFICACIÓN DE LAS GUÍAS DE USO, INSTALACIÓN Y CONFIGURACIÓN SEGURAS DEL TOE

3. Se incluirá una tabla en la que se identificarán las guías de uso, instalación y configuración que permiten operar al TOE en su configuración evaluada y certificada. Estas guías forman parte del TOE y se entregaran a los consumidores del producto.
4. En la tabla se incluirá al menos el nombre, versión y fecha de emisión de los documentos que constituyen las guías, o cualquier otro método que permita la identificación unívoca del documento como un resumen criptográfico del documento.

2.3 DESCRIPCIÓN DEL MODO DE USO DEL TOE (OPCIONAL)

5. Opcionalmente se podrá incluir una breve descripción del modo de uso del producto para cumplir con el objetivo de seguridad para el que fue diseñado.

3. ENTORNO DE EJECUCIÓN

3.1 DESCRIPCIÓN DEL ENTORNO DE EJECUCIÓN

6. La Declaración de Seguridad debe especificar el entorno operacional que se requiere para hacer posible la ejecución del producto. Este entorno puede ser de carácter genérico (por ejemplo, un ordenador con un sistema operativo determinado) o un entorno dedicado (Ej.- un ordenador con una configuración específica).
7. Cuando el entorno se describe de forma general, el evaluador no tiene la obligación de probar el producto en todas las plataformas posibles. Se debe de determinar una plataforma específica donde se llevará a cabo la evaluación. Esta especificación de la plataforma debe de aparecer de forma clara en el Informe Técnico de Evaluación y debe de ser indicada en el informe de certificación.

4. PROBLEMA DE SEGURIDAD

4.1 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN

8. La Declaración de Seguridad podrá incluir las hipótesis sobre el entorno en el que se ejecutará el producto, determinando el alcance de la evaluación. Dependiendo de las hipótesis que se declaren sobre el entorno de ejecución, el TOE puede verse limitado en su capacidad de proporcionar algunas las funcionalidades de seguridad declaradas al poder ser excluidos ciertos ataques al quedar limitado el escenario de ataque por dichas hipótesis.
9. Las posibles hipótesis sobre el entorno de ejecución pueden ser relativas a medidas de seguridad física, procedimentales, seguridad en el personal o seguridad lógica que se apliquen en el entorno de ejecución.
10. Por ejemplo, los ataques físicos quedarían fuera del alcance de la evaluación si se añadiese la siguiente hipótesis: “El TOE está protegido en una localización segura con acceso restringido a personas confiables. En particular, el atacante no tiene acceso físico al TOE”.

4.2 ACTIVOS SENSIBLES A PROTEGER

11. La Declaración de Seguridad debe describir los activos que las funciones de seguridad del TOE protegen. Deben especificarse las propiedades de seguridad que se protegen para cada uno de los activos (confidencialidad, integridad, disponibilidad, autenticidad y/o trazabilidad). Para proteger los activos enumerados, el producto puede hacer uso de otra información que deberá ser considerada un activo en sí misma. Por ejemplo, si la información de usuario es protegida en términos de confidencialidad por una función de cifrado que utiliza una clave concreta, dicha clave también se considera un activo sensible del TOE.

4.3 DESCRIPCIÓN DE LAS AMENAZAS

12. La Declaración de Seguridad debe describir las amenazas que se pretenden mitigar con las funciones de seguridad del TOE. Una amenaza se puede caracterizar con los siguientes elementos:
    i. Un actor (usuario autorizado, administrador, usuario malintencionado, atacante externo, etc.).
    ii. La acción adversa que ejecutaría el actor (inyección de datos, acceso malicioso, extracción de información, etc.).
    iii. El activo o activos a los que afectaría la acción adversa.
13. Por ejemplo, el hecho de que un usuario pueda inyectar información que modifique el comportamiento de una función de seguridad constituye una amenaza.

5. FUNCIONES DE SEGURIDAD

5.1 ESPECIFICACIÓN DE LAS FUNCIONES DE SEGURIDAD DEL PRODUCTO

14. La Declaración de Seguridad debe incluir una especificación de las funciones de seguridad que el producto implementa. Estas funciones deben especificarse en lenguaje natural. Pueden ser declaradas de forma explícita o referenciar a un estándar conocido que defina una funcionalidad de seguridad.

15. La especificación de las funciones de seguridad debe ser suficientemente completa como para que el evaluador entienda, sin lugar a dudas, cómo ha sido implementada la funcionalidad, es decir, se debe describir a alto nivel cómo el TOE proporciona la funcionalidad de seguridad. La especificación de las funciones de seguridad debe demostrar cómo cada una de las funciones contrarresta o mitiga las amenazas declaradas, por lo que al menos se incluirá una tabla resumen en la que se mapeen cada una de las funciones de seguridad declaradas con al menos una de las amenazas definidas en el problema de seguridad.

16. Cuando una Declaración de Seguridad hace referencia a un estándar, y este permite ser usado en base a diferentes parámetros, estos deben ser identificados de forma clara en la Declaración de Seguridad.

17. Si el estándar referenciado no proporciona la información requerida por este documento, la información adicional deberá ser especificada en la Declaración de Seguridad.

18. Las funciones de seguridad deben estar presentes en el modo de uso previsto del TOE y dentro del alcance de la certificación. Es decir, no se describirán las funciones de seguridad que no van a ser evaluadas y por lo tanto quedarán fuera del alcance de la certificación.

19. El fabricante puede no querer incluir en la Declaración de Seguridad información sensible o propietaria, ya que se trata de un documento público. En estos casos, es aceptable incluir con la entrega de la Declaración de Seguridad un documento anexo proporcionando el nivel de detalle esperado sobre la implementación de las funciones de seguridad sensibles o propietarias y referenciar a este anexo a lo largo de la Declaración de Seguridad. En todo caso, un consumidor del producto certificado tiene que ser capaz de conocer el alcance de la certificación del producto con la lectura de la Declaración de Seguridad, por lo que el laboratorio verificará que la información proporcionada en la Declaración de Seguridad permite conocer las funcionalidades de seguridad certificadas.

6. EVALUACIONES CON MÓDULOS OPCIONALES

6.1 (MEC) LISTADO DE MECANISMOS CRIPTOGRÁFICOS

20. Se incluirá un listado pormenorizado de los mecanismos criptográficos dentro del alcance de la evaluación criptográfica, incluyendo al menos el algoritmo, modo de funcionamiento y longitudes de clave. En el caso de que se empleen protocolos que hagan uso de funcionalidades criptográficas, como por ejemplo TLS, se deberá detallar también la versión o versiones del protocolo empleado y las *suites* criptográficas incluidas en el alcance. Este listado se encontrará detallado al menos en el epígrafe dedicado a la especificación de las funciones de seguridad.

6.2 (MCF) LISTADO DE MECANISMOS DE SEGURIDAD

21. Se incluirá un listado de los mecanismos de seguridad del TOE cuyo código fuente será evaluado. Este listado se encontrará detallado al menos en el epígrafe dedicado a la especificación de las funciones de seguridad.

6.3 (MEB) LISTADO DE MECANISMOS DE RECONOCIMIENTO BIOMÉTRICO

22. Se incluirá una descripción de los mecanismos y algoritmos de reconocimiento biométrico dentro del alcance de la evaluación biométrica. Este listado se encontrará detallado al menos en el epígrafe dedicado a la especificación de las funciones de seguridad.

7. REFERENCIAS

[CCN-STIC-2001] Definición de la Certificación Nacional Esencial de Seguridad (LINCE)

[CCN-STIC-2002] Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad (LINCE)

[CCN-STIC-2004] Plantilla del Informe Técnico de Evaluación de la Certificación Nacional Esencial de Seguridad (LINCE).

[CCN-STIC-140] Taxonomía de referencia para productos de Seguridad TIC

8. ACRÓNIMOS

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
ENS	Esquema Nacional de Seguridad
LINCE	Certificación Nacional Esencial de Seguridad
MCF	Módulo Revisión de Código Fuente
MEB	Módulo de Evaluación Biométrica
MEC	Módulo de Evaluación Criptográfica
ST	Security Target - Declaración de Seguridad
STIC	Seguridad de las Tecnologías de la Información y Comunicación
TIC	Tecnologías de la Información y Comunicación
TOE	Target Of Evaluation – Objeto a evaluar

PUBLICACIONES DE DEFENSA
GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL