centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 2004

Plantilla del Informe Técnico de Evaluación de la Certificación Nacional Esencial de Seguridad (LINCE)

Enero 2020

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

NIPO: 083-19-014-7

Fecha de Edición: Enero de 2020

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.02.10 10:57:25 +01'00'

CONTROL DE VERSIÓN

Versión	Comentario	Fecha
0.1	Versión en pruebas	Junio 2018

La presente versión de este documento se encuentra en fase de prueba en el ENESCTI. El Centro Criptológico Nacional acepta comentarios para la mejora de la presente edición de este documento. Puede proporcionar sus comentarios en la dirección de correo electrónico: organismo.certificacion@cni.es.

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

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

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 en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su 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, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, modificado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, 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 su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Julio de 2019

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

Este documento es una plantilla para redactar el Informe Técnico de Evaluación (ETR) de la Certificación Nacional Esencial de Seguridad (LINCE) del TOE.

Este documento establece la información que se debe incluir en el ETR.

Esta plantilla puede ser refinada de acuerdo al tipo de producto que deba evaluarse.

1.1 INFORMACIÓN DEL INFORME TÉCNICO DE EVALUACIÓN

Referencia ETR	Identificador único proporcionado por el laboratorio
Versión ETR	Versión del documento
Autor o autores	Nombre del autor del ETR
Aprobado por	Nombre del responsable del ETR
Fecha	Fecha de modificación del ETR
Código de expediente	Identificador único proporcionado por el CCN
Tipo de evaluación (incluir los módulos opcionales)	Ej.- LINCE + MEC + MCF
Taxonomía del producto según CCN-STIC 140	Ej.- HERRAMIENTAS ANTI-VIRUS/EPP (ENDPOINT PROTECTIONPLATFORM)

1.2 INFORMACIÓN DEL DESARROLLADOR Y DEL TOE

Datos del Patrocinador (Nombre y Dirección)	
Datos del Desarrollador (Nombre y Dirección)	
Datos de contacto del Desarrollador (Nombre del contacto y e-mail)	
Nombre del TOE	
Versión del TOE	

Manuales de uso del producto	

2. DESCRIPCIÓN DEL TOE

Para realizar un análisis de seguridad, el evaluador debe primero obtener conocimiento del TOE analizando la documentación disponible.

El evaluador debe posteriormente rellenar las siguientes secciones del Informe Técnico de Evaluación.

2.1 DESCRIPCIÓN FUNCIONAL DEL TOE

Esta sección consiste en la descripción del producto incluyendo en lenguaje natural sus componentes principales y las principales funciones de seguridad que implementa el mismo.

2.2 INVENTARIO DE LAS FUNCIONES DE SEGURIDAD IDENTIFICADAS EN LA DECLARACIÓN DE SEGURIDAD

Las funciones de seguridad listadas en la declaración de seguridad deben ser descritas y clasificadas por funcionalidad y se les debe asignar un identificador único que debe ser empleado a lo largo del informe para referenciar dicha funcionalidad.

(MEC) Se incluirá el listado de los mecanismos criptográficos del TOE dentro del alcance de la evaluación criptográfica.

(MCF) Se incluirá el listado de los mecanismos de seguridad del TOE cuyo código fuente ha sido evaluado.

3. ENTORNO DE EJECUCIÓN

3.1 DESCRIPCIÓN DEL ENTORNO DE EJECUCIÓN

Se debe especificar el entorno operacional que se requiere para hacer posible la ejecución del producto.

3.2 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN

Se deben incluir las hipótesis sobre el entorno en el que se ejecutará el producto y se les debe asignar un identificador único que debe ser empleado a lo largo del informe para referenciar dichas hipótesis.

4. RESUMEN EJECUTIVO DE LA EVALUACIÓN

El contenido esperado en este apartado consiste en realizar un resumen de la evaluación destacando los aspectos más importantes.

El objetivo es proporcionar una visión general de cómo se ha desarrollado la evaluación.

5. VEREDICTO DE LA EVALUACIÓN

El evaluador deberá asignar en el Informe Técnico de Evaluación un veredicto final para la evaluación de acuerdo a lo establecido en la metodología [CCN-STIC-2002]. Los posibles veredictos que se podrán asignar serán:

a) PASA: La funcionalidad de seguridad del TOE cumple con lo establecido en la Declaración de Seguridad y el TOE es resistente a un atacante con potencial de ataque bajo o moderado según lo establecido en esta metodología. En este caso el evaluador propondrá al Organismo de Certificación la resolución positiva del expediente de certificación.

b) FALLA: La funcionalidad de seguridad del TOE no cumple con lo establecido en la Declaración de Seguridad y/o el TOE no es resistente a un atacante con potencial de ataque moderado, es decir que el TOE se caracteriza por no tener un nivel de resistencia medio, según lo establecido en el apartado 4.5.1 de la metodología [CCN-STIC-2002]. También se asignará este veredicto si dentro del tiempo máximo de evaluación el patrocinador no ha proporcionado todas las evidencias necesarias establecidas en esta metodología. En este caso el evaluador propondrá al Organismo de Certificación la desestimación del expediente de certificación.

6. INSTALACIÓN DEL PRODUCTO

El contenido esperado en esta sección se encuentra detallado en la sección "Etapa 2 – Instalación del producto" del documento [CCN-STIC-2002].

La información que debe incluirse en esta sección es, como mínimo, la siguiente:

a) Evaluador o evaluadores encargados de esta actividad.

b) Descripción de la instalación y configuración del TOE y de las no-conformidades/acciones correctivas.

c) Configuración detallada del entorno de ejecución.

d) Opciones de instalación usadas.

e) Resultados de las tareas del evaluador indicadas en la sección "Etapa 2 – Instalación del producto" de la metodología [CCN-STIC-2002].

f) Tiempo dedicado instalar y configurar el TOE de acuerdo a las guías proporcionadas por el desarrollador.

7. ANÁLISIS DE CONFORMIDAD

7.1 ANÁLISIS DE LA DECLARACIÓN DE SEGURIDAD

El contenido esperado en esta sección se encuentra detallado en la sección "Etapa 1 – Análisis de la Declaración de Seguridad" del documento [CCN-STIC-2002].

La información que debe incluirse en esta sección es, como mínimo, la siguiente:

a) Evaluador o evaluadores encargados de esta actividad.

b) Referencia al identificador de la Declaración de Seguridad evaluada.

c) Resultados de las tareas del evaluador indicadas en la sección "Etapa 1 – Análisis de la Declaración de Seguridad" de la metodología [CCN-STIC-2002].

d) No conformidades encontradas.

e) Tiempo usado para el análisis.

7.2 ANÁLISIS DE LA DOCUMENTACIÓN

El contenido esperado en esta sección se encuentra detallado en la sección "Etapa 3 – Análisis de conformidad – análisis de la documentación" del documento [CCN-STIC-2002].

La información que debe incluirse en esta sección es, como mínimo, la siguiente:

f) Evaluador o evaluadores encargados de esta actividad.

g) Documentos analizados.

h) Aproximación utilizada para realizar el análisis.

i) Resultados de las tareas del evaluador indicadas en la sección "Etapa 3 – Análisis de conformidad – análisis de la documentación" de la metodología [CCN-STIC-2002].

j) No conformidades encontradas.

k) Tiempo usado para el análisis.

7.3 FUNCIONALIDADES PROBADAS

El contenido esperado en esta sección se encuentra detallado en la sección "Etapa 4 – Análisis de conformidad – Pruebas Funcionales" del documento [CCN-STIC-2002].

La información que debe incluirse en esta sección es, como mínimo, la siguiente:

a) Evaluador o evaluadores encargados de esta actividad

b) Justificación de la muestra utilizada

c) Información de cada test

d) No conformidades encontradas y sus resultados asociados

e) Tiempo usado para las pruebas

Para cada función probada, el evaluador deber rellenar la siguiente plantilla de "Caso de Prueba":

Código de la prueba:	(Ej.- TEST_0xx)	
Función de seguridad probada:	Evaluador:	
	Objetivo de la prueba:	
Escenario de prueba:		
Procedimiento	**Resultados esperados**	**Resultados obtenidos**
Conclusión y veredicto:		

Ejemplo:

Código de la prueba:		
Función de seguridad probada: Identificación de ataque	Evaluador: D.XX	
	Objeto de la prueba: Un detector de intrusiones debe de ser capaz de detectar ataques conocidos y debería disponer de las firmas/reglas necesarias para ello.	
Escenario de prueba: máquina recién instalada		
Procedimiento	**Resultados esperados**	**Resultados obtenidos**
Se realizará un ataque al servicio Apache 1.3.20 aprovechando la vulnerabilidad conocida. Para ello se habilitará una máquina externa que lanzará el ataque de	El IDS debe de detectar cuando el ataque se ha producido con marcas de tiempo similares a las de la máquina atacante.	Se puede observar en la información proporcionada por el IDS que se han detectado todos los ataques lanzados, pero, en algunos casos, con retardos

forma periódica.		considerables.

Conclusión y veredicto:

Los resultados son correctos, pero se precisa una optimización del procesamiento y el conjunto de reglas del detector de intrusiones con el fin de mejorar el tiempo de respuesta frente a ataques.

8. ANÁLISIS DE VULNERABILIDADES

El contenido esperado en esta sección se encuentra detallado en la sección "Etapa 5 – Análisis de vulnerabilidades" del documento [CCN-STIC-2002].

La información que debe incluirse en esta sección es, como mínimo, la siguiente:

a) Evaluador o evaluadores encargados de esta actividad.

b) Metodología utilizada para realizar el análisis de vulnerabilidades.

c) Análisis de vulnerabilidades del TOE (Proceso, Herramientas usadas, mecanismos analizados, etc.).

d) Listado de vulnerabilidades potenciales del producto junto con el análisis de la resistencia de los mecanismos/funciones como se especifica en la sección 4.5.1 de la metodología [CCN-STIC-2002].

e) Si el *(MCF)* está en el alcance, vulnerabilidades detectadas de la revisión de código fuente.

f) No conformidades encontradas.

g) Tiempo usado para el análisis.

9. *(MCF)* REVISIÓN DE CÓDIGO FUENTE

El contenido esperado en esta sección se encuentra detallado en la sección "4.5.2. Revisión de Código Fuente (MCF)" del documento [CCN-STIC-2002].

Esta sección no se incluirá en el ETR si el módulo MCF no es incluido en el alcance de la evaluación.

La información que debe incluirse en esta sección es, como mínimo, la siguiente:

a) Evaluador o evaluadores encargados de esta actividad.

b) Metodología utilizada para realizar la revisión del código fuente.

c) Listado de los mecanismos cuyo código fuente ha sido analizado y resultados de pruebas realizadas.

d) No conformidades encontradas y sus resultados asociados.

e) Tiempo usado para la revisión del código fuente.

10. *(MEC)* EVALUACIÓN CRIPTOGRÁFICA

El contenido esperado en esta sección se encuentra detallado en la sección "4.5.3. Evaluación Criptográfica (MEC)" del documento [CCN-STIC-2002].

Esta sección no se incluirá en el ETR si el módulo MEC no es incluido en el alcance de la evaluación.

La información que debe incluirse en esta sección es, como mínimo, la siguiente:

a) Evaluador o evaluadores encargados de esta actividad.

b) Metodología utilizada para realizar la evaluación criptográfica.

c) Listado y resultados de pruebas realizadas conforme a las tareas del evaluador detalladas en la sección "4.5.3. Evaluación Criptográfica (MEC)" de la metodología [CCN-STIC-2002].

d) No conformidades encontradas y sus resultados asociados.

e) Tiempo usado para la evaluación criptográfica.

11. PRUEBAS DE PENETRACIÓN DEL TOE

El contenido esperado en esta sección se encuentra detallado en la sección "Etapa 6 – Pruebas de penetración del TOE" del documento [CCN-STIC-2002].

La información que debe incluirse en esta sección es, como mínimo, la siguiente:

a) Evaluador o evaluadores encargados de esta actividad.

b) Listado de los test de penetración incluyendo al menos los pasos necesarios para reproducir la prueba, el resultado esperado, el resultado obtenido, y si el ataque tiene éxito o no.

c) No conformidades encontradas y sus resultados asociados.

d) Tiempo usado para realizar las pruebas de penetración.

Para cada prueba de penetración realizada, el evaluador deber rellenar la siguiente plantilla de "Caso de Prueba":

Código de la prueba:	(Ej.- TEST_0xx)	
Función de seguridad probada:	Evaluador: Objetivo de la prueba:	
Escenario de prueba:		
Procedimiento	**Resultados esperados**	**Resultados obtenidos**
Conclusión y veredicto:		

12. REFERENCIAS

[CC]	Common Criteria for Information Technology Security Evaluation. Se debe considerar su última versión aprobada y publicada en la web de Organismo de Certificación. (hhtps://oc.ccn.cni.es)
[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-807]	Criptología de empleo en el Esquema Nacional de Seguridad
[CEM]	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology. Se debe considerar su última versión aprobada y publicada en la web de Organismo de Certificación. (hhtps://oc.ccn.cni.es)

13. ACRÓNIMOS

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
ENS	Esquema Nacional de Seguridad
IDS	Intrusion Detection System – Sistema de Detección de Intrusiones
LINCE	Certificación Nacional Esencial de Seguridad (LINCE)
MCF	Módulo Revisión de Código Fuente
MEC	Módulo de Evaluación Criptográfica
STIC	Seguridad de las Tecnologías de la Información y Comunicación
TIC	Tecnologías de la Información y Comunicación
TOE	Target Of Evaluation – Objeto a evaluar