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)

Enero 2020

MINISTERIO DE DEFENSA

Edita:

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 10:56:26 +01'00'

NIPO: 083-19-013-1

Fecha de Edición: Enero de 2020

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 la Declaración de Seguridad del producto para la Certificación Nacional Esencial de Seguridad.

1.1 INFORMACIÓN DEL PATROCINADOR, TOE Y EVALUACIÓN

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	
Tipo de evaluación (incluir los módulos opcionales)	Ej.- LINCE + MEC + MCF
Manuales de uso del producto y su versión	
Taxonomía del producto según CCN-STIC-140	Ej.- HERRAMIENTAS ANTI-VIRUS/EPP (ENDPOINT PROTECTIONPLATFORM)

1.2 METODOLOGÍA Y CRITERIOS DE EVALUACIÓN

CCN-STIC-2001	CCN-STIC-2001 - Definición de la Certificación Nacional Esencial de Seguridad
CCN-STIC-2002	CCN-STIC-2002 - Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad
…	….

2. DESCRIPCIÓN DEL TOE

2.1 DESCRIPCIÓN FUNCIONAL DEL TOE

Una descripción del TOE incluyendo en lenguaje natural sus componentes principales y las principales funciones de seguridad que implementa el mismo.

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

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.

En la tabla se incluirá al menos el nombre, su versión y fecha de emisión de los documentos que constituyen las guías.

2.3 DESCRIPCIÓN DEL MODO DE USO DEL TOE (OPCIONAL)

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

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).

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

La Declaración de Seguridad debe incluir las hipótesis sobre el entorno en el que se ejecutará el producto. Esto determinará el alcance de la evaluación, puesto que dependiendo de las hipótesis que se realicen algunos posibles ataques pueden quedar fuera del alcance de la evaluación.

Ej.- Añadiendo esta 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"; los ataques físicos quedan fuera del alcance de la evaluación.

4.2 ACTIVOS SENSIBLES A PROTEGER

La Declaración de Seguridad debe describir los activos que las funciones de seguridad del TOE protegen. Debe especificarse la dimensión o dimensiones de seguridad que se protegen para cada uno de los activos (confidencialidad, integridad, disponibilidad, autenticidad). 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 confidencialidad de la información de usuario es protegida en términos de confidencialidad por una función de cifrado que utiliza una clave de cifrado concreta, dicha clave también se considera un activo sensible del TOE.

4.3 DESCRIPCIÓN DE LAS AMENAZAS

La Declaración de Seguridad debe describir las amenazas mitigadas por las funciones de seguridad. 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.

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

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

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.

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.

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

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.

La especificación de las funciones de seguridad debe demostrar cómo cada una de las funciones contrarresta o mitiga las amenazas declaradas.

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

La Declaración de Seguridad incluirá un listado de los mecanismos criptográficos del TOE dentro del alcance de la evaluación criptográfica.

6.2 (MCF) LISTADO DE MECANISMOS DE SEGURIDAD

La Declaración de Seguridad incluirá un listado de los mecanismos de seguridad del TOE cuyo código fuente será evaluado.

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
MEC	Módulo de Evaluación Criptográfica
ST	Security Target - Declaración de SeguridadDeclaración 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