centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 2002

Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad (LINCE)

Enero 2020

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

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 10:55:11 +01'00'

NIPO: 083-19-012-6

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. OBJETO DEL DOCUMENTO

Este documento establece la metodología de evaluación que se debe seguir durante la Certificación Nacional Esencial de Seguridad (LINCE).

2. OBJETIVO DE LA METODOLOGÍA

La metodología ha sido diseñada por el Centro Criptológico Nacional (CCN) con el objetivo de definir los pasos necesarios para realizar una evaluación de seguridad básica de productos IT.

La metodología de evaluación LINCE pretende dar respuesta a la necesidad de certificación de productos cuyo despliegue está previsto en entornos en los cuales el nivel de amenaza es de tipo básico o medio. Para los casos en los que el nivel de amenaza sea más elevado, sigue siendo recomendable que se empleen metodologías de evaluación formales como Common Criteria [CC], en las que el evaluador y certificador cuentan con mayor conocimiento sobre la correcta implementación de los mecanismos de seguridad del producto a certificar y se dedica un mayor esfuerzo en el proceso de certificación.

Esta evaluación comprende un alcance limitado dentro de un tiempo y esfuerzo acotado, permitiendo que los costes sean accesibles a todo tipo de fabricantes. Es por tanto, una metodología creada para la evaluación de productos de criticidad media o baja.

El objetivo del proceso de evaluación es permitir a un laboratorio de evaluación verificar si el producto es conforme a su especificación, determinando la efectividad de las funciones de seguridad implementadas e incluyendo los resultados en el Informe Técnico de Evaluación (ETR, Evaluation Technical Report).

Para hacerlo, el laboratorio de evaluación se basa en la Declaración de Seguridad (ST, Security Target) que define el alcance de la certificación, guías de uso y configuración segura del producto y la información pública del producto (especificaciones técnicas, fichas de producto, etc.), así como el producto propiamente dicho (TOE). Todos estos elementos serán proporcionados por el desarrollador del producto.

Adicionalmente para realizar el proceso de evaluación, el laboratorio empleará toda la información pública en relación al TOE a la que pueda tener acceso, como por ejemplo información publicada por el fabricante para ese producto o similares, información pública proporcionada por terceros en relación al producto o bases de datos públicas de vulnerabilidades de productos.

El papel que desempeñan durante el proceso de evaluación los distintos actores involucrados se describe en el documento [CCN-STIC-2001].

3. EVIDENCIAS MÍNIMAS NECESARIAS

El fabricante deberá proporcionar las evidencias incluidas en esta sección al inicio del proceso de evaluación.

Todas las evidencias deben de ser entregadas antes de que se inicie el proceso de evaluación. Esta medida es necesaria para cumplir con las limitaciones de tiempo establecidas.

A continuación, se proporciona el listado de evidencias obligatorias mínimas:

a) Declaración de Seguridad (ST)

b) Guías de operación e instalación del TOE

c) Entorno de ejecución del TOE

d) *(MCF) Módulo de Revisión de Código Fuente*: El código fuente de los mecanismos de seguridad del TOE declarados en el alcance de la Declaración de Seguridad para este módulo.

   Nota: A lo largo del documento se empleará la convención *(MCF)*, para identificar los requisitos opcionales de este módulo.

e) *(MEC) Módulo de Evaluación Criptográfica*: La documentación relacionada con los mecanismos criptográficos declarados en el alcance de este módulo y los mecanismos que permitan el acceso para probar la funcionalidad criptográfica.

   Nota: A lo largo del documento se empleará la convención *(MEC)*, para identificar los requisitos opcionales de este módulo

3.1 DECLARACIÓN DE SEGURIDAD

La Declaración de Seguridad (ST) se utiliza para especificar la funcionalidad de seguridad del producto que será evaluado y para describir las distintas relaciones entre el producto y el entorno en el cual será utilizado. La Declaración de Seguridad es importante para el desarrollador del producto y para el personal encargado de la evaluación, pero sobre todo es de especial interés para el personal responsable de la gestión, venta, instalación, configuración y uso del mismo. La ST define el alcance del certificado del producto y se publicará en conjunto con el certificado y el informe de certificación.

De acuerdo con la Plantilla de la Declaración de Seguridad [CCN-STIC-2003], la ST de un producto IT debe incluir la siguiente información:

a) Identificación unívoca y clara del TOE y sus guías y procedimientos de empleo seguro: El nombre del TOE y la versión concreta evaluada.

b) Información del TOE, describiendo claramente:

i. Descripción general del TOE incluyendo la funcionalidad de seguridad del mismo.

ii. El entorno de ejecución del TOE (Ej.- Sistema operativo donde se ejecuta el TOE, componentes externos necesarios para el correcto funcionamiento del TOE, etc.).

iii. Los activos sensibles que el TOE debe proteger.

iv. Las amenazas a las que el TOE debe hacer frente.

v. Las hipótesis sobre el entorno operacional que se tienen en cuenta para realizar la evaluación.

vi. Las funciones de seguridad implementadas por el TOE para contrarrestar las amenazas identificadas. Estas funciones serán objeto de evaluación.

vii. La identificación de las guías de configuración y uso seguro del producto.

Cada uno de los elementos listados se describe en mayor detalle a continuación:

a) Identificación unívoca y clara del TOE

Debe ser posible identificar sin ambigüedad el producto que está siendo evaluado y, en particular, su versión.

b) Identificación unívoca de las guías de operación o procedimientos de uso seguro y guías de instalación

Debe ser posible identificar sin ambigüedad las guías y procedimientos de uso seguro que van a ser o han sido empleados en la evaluación del producto, en particular, su versión y fecha de emisión.

c) Descripción del TOE

La Declaración de Seguridad debe describir el producto incluyendo en lenguaje natural sus componentes principales, las principales funciones de seguridad que implementa, así como el uso esperado del mismo.

d) 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 (por ejemplo, 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. En

este caso se debe determinar una plataforma específica donde se llevará a cabo la evaluación. Esta especificación de la plataforma aparecerá de forma clara en el Informe Técnico de Evaluación (ETR) y debe ser indicada en el informe de certificación.

e) Activos sensibles que deben de ser protegidos

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.

f) 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.

f) Especificación de las funciones de seguridad

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.

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 ST.

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.

g) *(MEC)* La Declaración de Seguridad incluirá un listado de los mecanismos criptográficos dentro del alcance de la evaluación criptográfica. Este listado se encontrará detallado al menos en el epígrafe dedicado a la especificación de las funciones de seguridad.

h) *(MCF)* La Declaración de Seguridad 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.

3.2 GUÍAS DE OPERACIÓN E INSTALACIÓN DEL TOE

El fabricante debe proporcionar las guías o manuales relacionadas con la operación e instalación del producto de manera segura y que servirán como base para la evaluación.

En las **guías de operación o procedimientos de empleo seguro**, el fabricante debe describir al menos:

a) Cómo usar de manera segura el TOE.

b) La funcionalidad accesible para cada rol de usuario.

c) Los parámetros seguros configurables por el usuario a utilizar durante la operación del TOE.

La documentación destinada a los usuarios debe describir las funciones de seguridad que conciernen al usuario final, así como proporcionar directrices suficientes para su funcionamiento seguro. Los manuales de referencias y guías de usuario deben estar bien estructurados, mantener una consistencia interna y no contradecirse con el resto de los documentos proporcionados al usuario final.

La documentación destinada a los administradores debe explicar cómo se administra el producto de forma segura, describiendo las funciones de seguridad que atañen al usuario administrador. Si se requiere un administrador, debe describir todos los parámetros de seguridad que están bajo su responsabilidad. Deberá describir todos los sucesos relacionados con la seguridad cubiertos por las funciones de administración, así como describir todos los procedimientos de seguridad cubiertos por la administración con un nivel de detalle que permita su uso sin errores. La documentación de administración debe proporcionar directrices para el uso coherente y eficaz de las características de seguridad del producto declaradas en la ST teniendo en cuenta la forma en que estas características interactúan. La documentación de administración, por ejemplo, los manuales de referencia y las guías del administrador, deben estar bien estructurados, mantener una consistencia interna y no contradecirse con los demás documentos que se proporcionan a los usuarios administradores.

En la **guía de instalación**, el fabricante debe describir los pasos necesarios para la instalación y configuración segura del producto. Esta documentación incluirá suficiente información para permitir realizar la instalación satisfactoriamente.

Si es posible realizar diferentes configuraciones, debe describirse el impacto de estas configuraciones en la seguridad. Esto implica la necesidad de revisar la documentación correspondiente a las distintas configuraciones del producto para su funcionamiento.

Deberán describirse los procedimientos para garantizar una puesta en marcha y un funcionamiento seguro. Si una función de seguridad puede ser desactivada o modificada durante la puesta en marcha, el funcionamiento normal o el mantenimiento del TOE, este hecho debe describirse. Si el producto contiene componentes de hardware de seguridad, debe haber funciones de diagnóstico implementadas que puedan ser ejecutadas por el administrador, el usuario final o de forma automática para verificar el correcto funcionamiento del producto en su entorno operativo.

Tanto las guías de operación como de instalación serán empleadas y verificadas por el laboratorio evaluador para llevar al TOE a su estado de operación seguro.

Únicamente las configuraciones detalladas en estas guías serán las configuraciones evaluadas y certificadas del TOE, por lo tanto el nivel de garantía proporcionado por el certificado está vinculado exclusivamente a la configuración evaluada. Las referencias univocas de estas guías deberán ser incluidas en la Declaración de Seguridad del fabricante. El evaluador deberá verificar que se puede realizar la puesta en marcha de cada una de las configuraciones del TOE descritas en la declaración de seguridad.

3.3 ENTORNO DE PRUEBAS PARA LA EJECUCIÓN DEL TOE

El fabricante proporcionará el entorno de pruebas del TOE al laboratorio. El entorno de pruebas deberá ser el necesario para poder probar toda la funcionalidad de seguridad definida en la Declaración de Seguridad en el entorno operativo descrito.

El laboratorio solicitará el comienzo de la evaluación una vez disponga del entorno de pruebas desplegado en sus instalaciones de forma que le permita comenzar con las tareas de evaluación solicitadas.

3.4 *(MCF)* EVALUACIÓN DE CÓDIGO FUENTE

El fabricante proporcionará el código fuente o implementación del TOE si el Módulo Código Fuente ha sido seleccionado como parte de la evaluación. Esto permite evaluar el producto con mayor grado de profundidad al realizarse una evaluación de "Caja blanca" con respecto a las funcionalidades para las que proporciona el código fuente o implementación del TOE.

El fabricante detallará en la Declaración de Seguridad las funcionalidades de seguridad que serán evaluadas mediante el Módulo Código Fuente. Estas funcionalidades también serán detalladas en el informe de certificación.

Los certificados que empleen este módulo opcional serán identificadas como LINCE + MCF, de forma que se pueda identificar qué partes de su funcionalidad de seguridad han sido evaluadas teniendo en cuenta su implementación.

3.5 *(MEC)* EVALUACIÓN DE LOS MECANISMOS CRIPTOGRÁFICOS

El fabricante proporcionará la información de la implementación de los mecanismos criptográficos si el Módulo Criptográfico ha sido seleccionado como parte de la evaluación.

El fabricante detallará en la Declaración de Seguridad los algoritmos criptográficos que serán evaluados mediante el Módulo Criptográfico. Estos algoritmos también serán detallados en el informe de certificación.

La información relacionada con los mecanismos criptográficos debe incluir:

a) La descripción de las funciones criptográficas que proporciona el producto (cifrado, firma, gestión de claves, etc.).

b) La referencia de los algoritmos a estándares inequívocos, reconocidos, y cuyos detalles técnicos sean accesibles fácilmente y sin condiciones, junto con los parámetros y procedimientos para su implementación.

La información relacionada con la gestión de claves debe incluir:

a) El tamaño de clave.

b) El modo de distribución de claves.

c) El proceso de generación de claves.

d) El proceso de borrado de claves

e) El mecanismo, formato y lugar de almacenamiento de claves.

f) El mecanismo de transporte de claves.

La información relacionada con el procesamiento de datos debe incluir la descripción del procesamiento que se realiza en los datos antes o después de la operación criptográfica (compresión, formato, adición de una cabecera, etc.).

Cuando se usa un generador de números aleatorios para implementar funciones criptográficas, deberá describirse el tipo, el método y arquitectura usados, incluyendo las justificaciones necesarias que demuestren que el generador de números aleatorios se considera efectivo.

Adicionalmente a este documento, el evaluador debe disponer de acceso a dichos mecanismos criptográficos con la finalidad de comprobar la funcionalidad criptográfica.

Para cumplir este último requisito, podrá ser necesario que el fabricante proporcione versiones modificadas del producto que permitan el acceso directo a la funcionalidad criptográfica a través de una interfaz programable que permita al evaluador verificar la correcta implementación de la misma.

Los certificados que empleen este módulo opcional serán identificadas como LINCE + MEC, de forma que se pueda identificar qué algoritmos han sido evaluados teniendo en cuenta su implementación.

4. PROCEDIMIENTO DE EVALUACIÓN

Este capítulo establece el criterio de evaluación con el cual se pretende verificar la conformidad y la resistencia de la funcionalidad de seguridad del producto.

La metodología está fuertemente basada en los niveles básicos de [CC] y [CEM]. Por lo tanto, se pueden considerar documentos de apoyo a la metodología de evaluación para la Certificación Nacional Esencial de Seguridad (LINCE).

A continuación, se describen las distintas etapas a realizar como parte de la evaluación.

4.1 ETAPA 1 – ANÁLISIS DE LA DECLARACIÓN DE SEGURIDAD

Tareas del evaluador

1.1. Comprobar que la Declaración de Seguridad contiene los elementos descritos en el capítulo 3.1 de este documento y en [CCN-STIC-2003].

1.2. Comprobar que la descripción del TOE no es confusa y que describe al menos la funcionalidad mínima para la que está diseñado.

1.3. Comprobar que existe una correcta delimitación de las partes que pertenecen al TOE y las partes que pertenecen al entorno operacional, así como una adecuada descripción de cómo el entorno operacional da soporte a la ejecución del TOE.

1.4. Comprobar que las funciones de seguridad mitigan o contrarrestan las amenazas descritas en la declaración de seguridad.

1.5. Comprobar que cada una de las funciones de seguridad está relacionada con una o varias de las amenazas incluidas en la declaración de seguridad.

1.6. Comprobar que las hipótesis del entorno son relevantes en relación a las amenazas y el uso para el cual el producto fue diseñado.

1.7. Comprobar que las funciones de seguridad se describen al nivel de detalle necesario para permitir al evaluador entender cómo las funciones de seguridad están implementadas por el TOE.

1.8. En el caso de declarar módulos opcionales *(MCF)* o *(MEC)*, comprobar que se detallan las funcionalidades que se verificarán como parte de la evaluación con estos módulos opcionales.

4.2 ETAPA 2 – INSTALACIÓN DEL PRODUCTO

Tareas del evaluador

2.1. Comprobar que, de acuerdo con las guías de instalación o configuración del producto, es posible instalar el producto de acuerdo a la configuración o configuraciones descritas en la Declaración de Seguridad.

- En el caso de los productos que puedan instalarse en varias versiones del sistema operativo, debe indicarse el sistema operativo utilizado y su versión, con la máxima precisión posible (parche, *service pack*, etc.).
- Si el producto requiere instalación, se instalará el producto en su configuración típica. Adicionalmente el fabricante proporcionará la documentación relacionada con los distintos modos de configuración existentes en el producto.

2.2. Comprobar que el fabricante ha proporcionado la plataforma de pruebas requerida para llevar a cabo las pruebas en el producto.

2.3. Registrar la información relevante que permite que la instalación se desarrolle satisfactoriamente.

2.4. Registrar todos los datos específicos de la configuración del sistema, cuando corresponda.

2.5. Indicar todas las no-conformidades en relación con la instalación y configuración del TOE o del entorno de pruebas.

Nota: El fabricante debe asistir al evaluador, si es necesario, en la instalación del TOE y en la configuración del entorno de pruebas. Dada la limitación temporal de la evaluación, el evaluador debe centrar los esfuerzos en el análisis y pruebas del producto, por tanto, se requiere la asistencia del fabricante para esta tarea.

4.3 ETAPA 3 – ANÁLISIS DE CONFORMIDAD – ANÁLISIS DE LA DOCUMENTACIÓN

Tareas del evaluador

3.1. Listar los documentos analizados.

3.2. Comprobar que la información proporcionada cumple los requisitos relacionados con el contenido y la presentación (Sección 3), proporcionando un veredicto sobre su completitud y legibilidad. Si existe un gran volumen de documentación a revisar, el evaluador podrá, previa notificación al Organismo de Certificación, operar por muestreo, de acuerdo con el siguiente orden de prioridades:

a) La Declaración de Seguridad proporcionada por el fabricante;

b) Guías de operación e instalación del TOE;

3.3. Indicar todas las no-conformidades en relación con cualquier documentación existente.

4.4 ETAPA 4 – ANÁLISIS DE CONFORMIDAD –PRUEBAS FUNCIONALES

Tareas del evaluador

4.1. Revisar y probar las funciones de seguridad del producto con una profundidad que permita comprobar que la funcionalidad de seguridad declarada en la Declaración de Seguridad por el fabricante ha sido implementada en el producto.

Si las pruebas no son completas, el evaluador debe justificar la muestra realizada. Para cada una de las pruebas realizadas, el evaluador deberá proporcionar la siguiente información:

a) La funcionalidad probada

b) El escenario de pruebas

c) El procedimiento con los pasos a seguir

d) Los resultados esperados y obtenidos

e) Conclusión y veredicto de la prueba

Ver sección 7.2 de [CCN-STIC-2004] para más información.

4.2. Indicar todas las no-conformidades en relación con cualquier prueba realizada.

Nota: El evaluador puede seguir las guías dadas en [CEM] para la realización de las pruebas independientes.

4.5 ETAPA 5 – ANÁLISIS DE VULNERABILIDADES

El evaluador debe seguir las guías proporcionadas en [CEM] para la realización de un análisis de vulnerabilidades, cuyo propósito es determinar la existencia y, en su caso, explotabilidad de los fallos y debilidades del TOE en el entorno operacional.

Dada la limitación en tiempo y esfuerzo de la certificación, el evaluador podrá solicitar la realización de sesiones de trabajo con el fabricante para ganar conocimiento del TOE de la manera más rápida posible.

Tareas del evaluador

5.1. Realizar un análisis metódico en la búsqueda de vulnerabilidades utilizando todos los medios que tenga a su alcance, usando al menos las siguientes fuentes de información:

a) La documentación proporcionada por el fabricante (Ej.- Declaración de seguridad, guías de usuario, etc.).

b) Información disponible sobre la tecnología.

c) Las bases de datos de vulnerabilidades públicas para el tipo del producto.

d) El producto en sí mismo, el cual está instalado en una plataforma de pruebas lo más representativa posible con respecto al entorno de ejecución del producto.

5.2. Documentar el método utilizado para la búsqueda de vulnerabilidades y definir los ataques a realizar durante la fase de pruebas de penetración.

5.3. Documentar todas las vulnerabilidades potenciales encontradas.

4.5.1. ANALÍSIS DE LA RESISTENCIA DE LOS MECANISMOS/FUNCIONES

Para cada una de las vulnerabilidades potenciales encontradas por el evaluador, se realizará un estudio de la resistencia del TOE a este ataque. Es decir, el nivel de recursos que un atacante necesitaría para tener éxito en un ataque. A continuación se da información de cómo realizar este estudio:

El evaluador podrá requerir información adicional al fabricante para hacer un uso correcto del sistema de cálculo.

Tareas del evaluador

5.4. Calcular el potencial de ataque para cada vulnerabilidad potencial según el siguiente sistema de puntuación:

Las siguientes tablas muestran los datos principales que permiten realizar una valoración. El evaluador consultará la metodología [CEM] y/o al Organismo de Certificación en el caso de duda en la valoración del potencial de ataque.

Tabla 1 - Valoración de los factores de identificación y explotación de una vulnerabilidad

Factor	Intervalo	Valor para identificar una vulnerabilidad	Valor para explotar una vulnerabilidad
Tiempo necesario	< 1 hora	0	0
	< 1 día	2	3
	< 1 mes	3	5
	> 1 mes	5	8
	No práctico	*	*
Experiencia del atacante	Inexperto	0	0
	Competente	2	2

	Experto	5	4
Conocimiento necesario para el atacante	Ninguno	0	0
	Información pública	2	2
	Información sensible	5	4
Acceso al producto por el atacante	< 0.5 horas o directamente accesible	0	0
	< 1 día	2	4
	< 1 mes	3	6
	> 1 mes	4	9
	No práctico	*	*
Tipo de equipamiento necesario para identificar / explotar la vulnerabilidad	Ninguno	0	0
	Estándar	1	2
	Especializado	3	4
	Específico	5	6

Nota: * indica nivel de resistencia alto

Tabla 2 - Valoración del nivel de resistencia a la amenaza

Suma de los valores	Resistente a un atacante con un potencial de ataque	Nivel de resistencia
0 a 9	Sin clasificación	
10 a 17	Bajo	Básico
18 a 24	Moderado	Medio
>24	Alto	Alto

El nivel de resistencia se computará teniendo en cuenta la suma de los valores asignados por el laboratorio para las fases de identificación y explotación de la Tabla 1. Las vulnerabilidades con potencial de ataque mayor a 24 se consideran residuales.

4.5.2. REVISIÓN DE CÓDIGO FUENTE *(MCF)*

Si el Módulo Código Fuente es incluido, el evaluador podrá realizar una evaluación de caja blanca. Por lo tanto, la fase de análisis de vulnerabilidades se verá apoyada con esta evidencia.

Tareas del evaluador

MCF.1. Indicar el código fuente de las funcionalidades de seguridad que han sido analizadas conforme a lo declarado en la Declaración de Seguridad. Es posible proceder por muestreo, siempre y cuando este punto sea autorizado por el Organismo de Certificación y si el tamaño del código lo requiere. La estrategia de muestreo será documentada en el informe de evaluación (ETR).

MCF.2. Indicar las técnicas utilizadas para realizar la revisión de código fuente.

MCF.3. Indicar todas las no-conformidades en relación con cualquier deficiencia encontrada en el código.

4.5.3. EVALUACIÓN CRIPTOGRÁFICA *(MEC)*

La evaluación criptográfica se realizará cuando el solicitante de la certificación ha seleccionado el Módulo Criptográfico en su solicitud y ha identificado en la Declaración de Seguridad los mecanismos criptográficos objeto a evaluar mediante el Módulo Criptográfico.

El evaluador debe disponer de soporte técnico por parte del desarrollador para interpretar la información suministrada además de disponer de toda la información posible sobre los mecanismos criptográficos implementados en el producto.

Tareas del evaluador

MEC.1. Analizar la conformidad de los mecanismos criptográficos declarados con respecto a la guía [CCN-STIC-807] mediante análisis documental.

MEC.2. Verificar la implementación de estos mecanismos por el producto mediante alguna de las siguientes formas:

- Pruebas funcionales: Por comparación de los resultados del mecanismo criptográfico llevado a cabo por el producto en relación a la implementación de referencia. Más información en la sección 4.5.3.1.

Nota: Esto significa que el evaluador debe disponer de una implementación de referencia autorizada por el CCN.

- Análisis del código fuente con posibles pruebas unitarias en determinadas funciones, por ejemplo, para comprobar que una función AES realmente implementa AES.

MEC.3. Describir el enfoque adoptado para garantizar la conformidad de la aplicación con las especificaciones.

MEC.4. Si existen generadores de números aleatorios, comprobar que el generador cumple con los requisitos descritos en la guía del CCN [CCN-STIC-807]. Se indicará cualquier tipo de prueba que haya llevado a cabo para asegurar la naturaleza aleatoria de la fuente.

MEC.5. Indicar todas las no-conformidades en relación con cualquier debilidad o vulnerabilidad encontrada.

4.5.3.1. VERIFICACIÓN DE LA IMPLEMENTACIÓN MEDIANTE PRUEBAS FUNCIONALES

En esta sección, se proporcionan pautas para probar la funcionalidad criptográfica. Estas pruebas consisten en usar vectores de test, los cuales sean capaces de demostrar las funcionalidades esperadas por algún tipo concreto de algoritmo, con el fin de comprobar los mecanismos de seguridad que ofrece, tal y como se puede observar en el siguiente ejemplo propuesto.

En este caso se utilizará como ejemplo un posible producto, el cuál usa el algoritmo AES:

a) *"AES-CBC: existen cuatro pruebas posibles que deben ser superaras para verificar una correcta implementación del algoritmo y modo. Dichas pruebas se describen a continuación. Cabe tener en cuenta que, en todos estos test, el texto en claro, el texto cifrado y los valores de vectores de inicialización deben de ser de bloques de 128 bits.*

   i. *Test 0 – Para comprobar que las funcionalidades de los procesos de cifrado y de descifrado son una la inversa de la otra, el evaluador considerará un conjunto de diez textos claros de 128 bits, elegidos al azar. Cinco de ellos se cifrarán utilizando cinco claves aleatorias de 128 bits y los otros cinco con otras tantas claves aleatorias de 256 bits. En todos los casos se emplearán vectores de inicialización aleatorios. A continuación se procederá a descifrar los textos cifrados obtenidos, cada uno con su clave y su vector correspondiente, verificando que el resultado del descifrado es el texto claro de partida.*

   ii. *Test 1 – Para comprobar las funcionalidad del proceso de cifrado del AES-CBC, el evaluador debe considerar un conjunto de diez*

textos claros, elegidos al azar, y obtener los correspondientes textos cifrados. Para todos los procesos de cifrado se emplearán vectores de inicialización con todos sus valores a 0.

Por su parte, cinco de los textos claros se cifrarán con una clave de 128 bits, todos iguales a 0; y los restantes cinco textos claros se cifrarán con una clave de 256 bits, también todos a 0.

Para comprobar las funcionalidades del proceso de descifrado, se deben desarrollar las pruebas análogas que para el cifrado utilizando los mismos vectores de inicialización y las mismas claves, empleando en cada caso como entrada los textos cifrados obtenidos en los diez procesos de cifrado mencionados.

iii. *Test 2 – Para comprobar la funcionalidad del proceso de cifrado, se cifrarán diez textos claros con diez claves, generadas al azar, la mitad de las cuales serán de 128 bits y las restantes cinco de 256 bits.*

Tanto el vector de inicialización como los textos claros estarán compuestos exclusivamente por ceros.

Para probar la funcionalidad del proceso de descifrado, se realizarán pruebas similares a las anteriores, empleando para ello como entradas los correspondientes textos cifrados.

iv. *Test 3 – Para probar la funcionalidad del proceso de cifrado del algoritmo se deben crear dos conjuntos de claves, uno con claves de 128 bits y otro con claves de 256 bits. Las claves se construirán de la siguiente manera: La clave i-ésima de cada conjunto debe tener los i bits más a la izquierda (bits más significativos) iguales a 1 y restantes N-i bits más a la derecha (menos significativos) iguales a 0, donde i recorre el intervalo [1,N], siendo N el número de bits de la clave.*

Para cada clave se cifrará un texto claro compuesto solo por ceros y se empleará un vector de inicialización también compuesto solo por ceros.

Para probar la funcionalidad del proceso de descifrado del algoritmo se procederá de modo similar a como se acaba de mencionar, utilizando las mismas claves, los mismos vectores de inicialización y como textos cifrados los obtenidos en los procesos de cifrado anteriores.

v. *Test 4 – Para probar la funcionalidad del proceso de cifrado del algoritmo se debe crear un conjunto de textos claros de 128 bits de modo que el texto claro i-ésimo esté formado por los i bits más a la izquierda (bits más significativos) iguales a 1 y restantes 128-i bits más a la derecha (menos significativos) iguales a 0, donde i recorre el intervalo [1,128]. Además, se considerarán dos*

claves, una de 128 bits y otra de 256 bits, todos ellos iguales a 0. El vector de inicialización también estará compuesto solo por ceros. De este modo, cada texto claro dará lugar a dos textos cifrados, uno correspondiente a cada una de las dos claves.

Para probar la funcionalidad del proceso de descifrado del algoritmo se procederá de modo similar a como se acaba de mencionar, utilizando las mismas claves, los mismos vectores de inicialización y como textos cifrados los obtenidos en los procesos de cifrado anteriores.

Los resultados para cada prueba deben ser obtenidos por el evaluador con soporte del fabricante. El evaluador debe comparar los resultados con los de una implementación conocida correcta.

El Organismo de Certificación proporcionará las guías correspondientes para probar cada uno de los posibles algoritmos.

4.6 ETAPA 6 – PRUEBAS DE PENETRACIÓN DEL TOE

La finalidad de esta etapa es asegurar que un producto y sus características de seguridad son efectivas para contrarrestar amenazas de nivel básico y moderado, excluyendo por tanto aquellos ataques realizados por individuos u organizaciones con un potencial de ataque alto.

El evaluador intentará optimizar en la medida de lo posible los recursos utilizados y destinar el tiempo asignado a esta etapa a encontrar y realizar pruebas en el producto.

Por lo tanto, en el proceso de evaluación de un producto se deben realizar pruebas de penetración con el objetivo de:

- Confirmar la explotabilidad de las vulnerabilidades potenciales identificadas durante el análisis de vulnerabilidades
- Realizar nuevas pruebas con el fin de detectar vulnerabilidades nuevas o no conocidas/públicas del producto.

Estas pruebas de penetración serán de tipo Caja negra (salvo que el Módulo Código Fuente esté incluido en el alcance de la evaluación, en cuyo caso se probarán las funcionalidades declaradas dentro del Módulo Código Fuente con información sobre su implementación).

Tareas del evaluador

6.1. Proporcionar un listado de todas las pruebas de penetración realizadas en el TOE, incluyendo al menos, los pasos necesarios para reproducir la prueba, el resultado esperado, el resultado obtenido, y si el ataque tiene éxito o no.

6.2. Indicar todas las no-conformidades en relación con cualquier ataque que haya tenido éxito.

5. VEREDICTO DE LA EVALUACIÓN

La última etapa del proceso de evaluación es la asignación del veredicto final por parte del laboratorio. El veredicto será uno de los dos siguientes:

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 esta metodología (ver apartado 4.5.1). 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. RESTRICCIONES TEMPORALES Y DE ESFUERZO DE LA EVALUACIÓN

La evaluación se debe llevar a cabo bajo unas restricciones estrictas de tiempo y carga de trabajo, cuyo objetivo es limitar el esfuerzo y la duración del proceso.

Como norma general, una evaluación LINCE debe llevarse a cabo con una carga de trabajo estimada de **25 jornadas laborables de una persona** con un periodo de realización máximo de **8 semanas**.

Para la estimación de tiempos y esfuerzos, se ha considerado que los evaluadores tienen las capacidades y experiencia necesarias para realizar la evaluación del producto. El tiempo necesario para preparar a los evaluadores (Ej.- una tecnología nueva) no se ha tenido en cuenta.

Para los **módulos** opcionales (*MCF y MEC*), se añaden **5 jornadas** de esfuerzo y **2 semanas** de duración máxima adicionales para cada uno de los módulos.

Incluyendo los dos módulos, una certificación LINCE debe llevarse a cabo con un esfuerzo de 35 jornadas laborables por una persona y con una duración máxima de 12 semanas.

De acuerdo con esta temporización, en la siguiente imagen se puede observar una tabla de esfuerzos orientativa en función de cada etapa de la evaluación:

ACTIVIDAD	INICIO DEL PERIODO	DURACIÓN DEL PERIODO
Etapa 1 - Análisis de la declaración de seguridad	1	1
Etapa 2 - Instalación del producto	2	1
Etapa 3 - Análisis de conformidad - Análisis de la doc.	3	2
Etapa 4 - Análisis de conformidad - Pruebas funcionales	5	5
Etapa 5 - Análisis de conformidad - Análisis de vulnerabilidades	10	6
Etapa 5.1 - Revisión de Código Fuente	16	5
Etapa 6 - Evaluación Criptográfica	21	5
Etapa 7 - Test de penetración del TOE	26	10

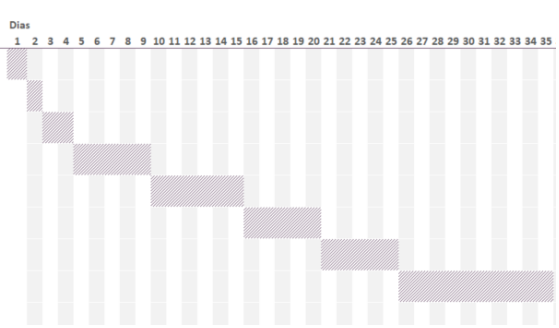

Ilustración 1. Diagrama de Gantt de la evaluación

7. RESULTADOS DE LA EVALUACIÓN

La evaluación de un producto de acuerdo con el criterio destacado en este documento debe comprobar que el TOE implementa las funciones de seguridad indicadas en la Declaración de Seguridad y que el TOE es resistente a atacantes con un potencial de ataque moderado. Esta conclusión final debe adoptarse con el debido cuidado dentro del ámbito de la seguridad TIC, dado que es técnicamente imposible garantizar que no habrá vulnerabilidades explotables en el producto.

El resultado de una evaluación LINCE será un informe técnico de evaluación (ETR) que contendrá al menos la siguiente información:

a) Un resumen de la evaluación realizada por parte del laboratorio incluyendo la aproximación utilizada para realizar la evaluación, el esfuerzo dedicado en cada actividad y el resultado del análisis de seguridad para cada función de seguridad declarada por el fabricante en la declaración de seguridad.

b) Una lista de las principales herramientas de análisis utilizadas.

c) Listado y descripción de las vulnerabilidades potenciales encontradas durante la evaluación del producto.

d) Listado y descripción de las vulnerabilidades explotadas en el producto.

e) Las correcciones realizadas en el producto para mitigar las vulnerabilidades explotadas, siempre que sea posible.

f) Un resumen de los resultados de las pruebas llevadas a cabo en el producto.

g) Veredicto y conclusiones de la evaluación.

La emisión de un ETR por parte del laboratorio es de obligado cumplimiento. El Informe Técnico de Evaluación elaborado por el evaluador, que contiene y presenta los resultados de la evaluación, debe contener la información requerida en la plantilla [CCN-STIC-2004]. Si el ETR muestra que el producto no cumple o solo cumple parcialmente su declaración de seguridad, se considerará que el producto no cumple su Declaración de Seguridad y por lo tanto se propondrá la desestimación de la certificación por parte del laboratorio.

8. GLOSARIO

Este apartado contiene las definiciones de los términos técnicos utilizados con un significado específico para este documento.

Acciones del evaluador: parte de los criterios de evaluación para una fase o un aspecto específico de la evaluación en la que se identifica lo que el evaluador debe hacer para comprobar la información proporcionada por el fabricante y las acciones complementarias que se deben llevar a cabo.

Administrador: persona en contacto con el producto y responsable del mantenimiento en el entorno operacional.

Amenaza: acción o evento que pueda afectar a la seguridad de un producto IT.

Certificación: emisión de una declaración formal por parte de un tercero independiente en la que se confirman los resultados de una evaluación y la correcta aplicación de los criterios de evaluación utilizados.

Confidencialidad: propiedad que garantiza que la información es accesible sólo para aquellos autorizados a tener acceso.

Configuración: selección de una de las posibles combinaciones de características/propiedades de un objeto a evaluar .

Declaración de seguridad: especificación de la funcionalidad de seguridad a evaluar de un TOE específico. También describirá las amenazas al TOE, los activos a proteger y los mecanismos de seguridad implementados por el TOE. Además, identificará unívocamente el objeto a evaluar y el alcance de la evaluación.

Desarrollador: persona o entidad que desarrolla, implementa o fabrica un objeto a evaluar.

Disponibilidad: característica de seguridad que asegura acceso a los recursos o información.

Documentación: información escrita (o información registrada de otro modo) relativa a un objeto de evaluación objeto a evaluar requerida para una evaluación. Esta información puede ser recogida en un documento individual y destinado para este propósito, pero no es obligatorio.

Eficacia: propiedad de un objeto de evaluación objeto a evaluar que representa como proporciona seguridad en el contexto de su uso real o previsto.

Entorno de ejecución: medidas procedimentales y elementos del entorno (Ej.- bases de datos, firewalls, etc.) necesarios para el correcto funcionamiento del TOE.

Evaluación: valoración por parte de un tercero independiente del grado de cumplimiento de un producto en relación con los criterios de evaluación definidos.

Evaluador: persona o entidad independiente que realiza una evaluación.

Garantía: confianza que puede concederse a los mecanismos de seguridad implementados en un objeto a evaluar.

Implementación: fase en el proceso de desarrollo en la cual la especificación detallada de un objeto de evaluación objeto a evaluar es trasladada al hardware y software. Ej.- código fuente

Integridad: propiedad que garantiza que la información es modificada sólo por aquellos autorizados.

Mecanismos de seguridad: lógica o algoritmo el cual implementa por hardware o software una función de seguridad específica.

Mecanismos de seguridad: lógica o algoritmo el cual implementa por hardware o software una función de seguridad específica o que contribuye a la seguridad.

Objeto a evaluar (TOE): producto que se somete a una evaluación de seguridad.

Operación: etapa de uso de un TOE.

Organismo de Certificación: organismo nacional, independiente e imparcial el cual se encarga de las certificaciones. Es el responsable de la emisión del certificados de seguridad TIC. En este caso se refiere al organismo creado por el RD421/2004 y regulado por la Orden PRE/2740/2007.

Patrocinador: persona u organismo que solicita y patrocina una certificación y evaluación.

Producto TIC: paquete software y/o hardware que implementa una funcionalidad TIC determinada.

Requisitos de contenido y presentación: parte de los criterios de evaluación para una etapa o aspecto específico de la evaluación que explique que debe contener cada elemento de la documentación identificado como parte de esta etapa o aspecto y como debe presentarse la información que contiene.

Seguridad: combinación de confidencialidad, integridad, disponibilidad, autenticación y no-repudio.

Test de penetración: pruebas llevadas a cabo por un evaluador en un TOE para confirmar si se identifican o no vulnerabilidades que puedan ser actualmente explotadas.

Usuario final: persona o entidad que opera el TOE en su entorno operacional.

Vulnerabilidades: debilidad de alguna de las características de seguridad declaradas para de un TOE en su Declaración de Seguridad (debido por ejemplo a fallos en el análisis, el diseño, fabricación u operación).

9. 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-2003] Plantilla para la Declaración de Seguridad de 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-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)

10. ACRÓNIMOS

AES Advanced Encryption Standard
CCN Centro Criptológico Nacional
CNI Centro Nacional de Inteligencia
ENS Esquema Nacional de Seguridad
ETR Evaluation Technical Report
IT Information Technology
LINCE Certificación Nacional Esencial de Seguridad (LINCE)
MCF Módulo Revisión de Código Fuente
MEC Módulo de Evaluación Criptográfica
RD Real Decreto
ST Security Target - Declaración de Seguridad
STIC Seguridad de las Tecnologías del a Información y Comunicación
TIC Tecnologías de la Información y Comunicación
TOE Target Of Evaluation – Objeto a evaluar