centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 2002

Metodología de Evaluación para 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 11:36:58 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-088-0

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. OBJETO DEL DOCUMENTO

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

2. OBJETIVO DE LA METODOLOGÍA

2. La metodología LINCE 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 TIC (Tecnologías de la Información y las Comunicaciones).

3. El Centro Criptológico Nacional ha desarrollado la metodología de evaluación y certificación LINCE como 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 sustancial de acuerdo al Cybersecurity Act (Reglamento (EU) 2019/881 del Parlamento Europeo y del Consejo del 17 de Abril 2019 sobre ENISA y sobre el marco europeo de certificación). Para los casos en los que el nivel de amenaza sea más elevado, sigue siendo recomendable que se empleen metodologías de evaluación como Common Criteria [CC], en las que tanto el evaluador como el certificador cuentan con un mayor conocimiento de la implementación de los mecanismos de seguridad del producto a certificar, se le dedica un mayor esfuerzo de evaluación y por lo tanto se obtiene un mayor nivel de garantía de seguridad sobre el producto certificado.

4. Esta evaluación comprende un alcance limitado dentro de un tiempo y esfuerzo acotado y está orientada a la verificación de funcionalidad de seguridad y análisis de vulnerabilidades mediante pruebas funcionales y de penetración. Este enfoque, permite que los costes sean accesibles a todo tipo de fabricantes. Teniendo en cuenta el alcance limitado, esta metodología se crea para la evaluación de productos de criticidad media o baja.

5. 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*).

6. 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.

7. 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.

8. 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

9. El solicitante deberá proporcionar las evidencias que se indican en esta sección antes de que se inicie el proceso de evaluación. Esta medida es necesaria para cumplir con las limitaciones de tiempo establecidas.

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

    a) Declaración de Seguridad (ST)

    b) Guías de instalación, configuración y operación del TOE

    c) Entorno de ejecución del TOE, incluyendo todos los elementos hardware y software necesarios que permitan desplegar el TOE en la configuración que se pretende evaluar.

    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/herramientas 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

    f) *(MEB) Módulo de Evaluación Biométrica*: La documentación relacionada con la funcionalidad y algoritmos de reconocimiento biométrico declarados en el alcance de este módulo, así como los mecanismos que permitan el acceso para probarla.

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

3.1 DECLARACIÓN DE SEGURIDAD

11. 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.

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

    a) Identificación unívoca y clara del TOE: el nombre del TOE y la versión concreta evaluada.

    b) (Opcional) Identificación de la taxonomía del producto según la guía CCN-STIC-140.

    c) Tipo de evaluación (ej. LINCE + MCF)

    d) Identificación de las guías de operación e instalación/configuración.

    e) Información del TOE, describiendo claramente:

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

        ii. Las guías de instalación, configuración y operación, incluyendo como mínimo el nombre y la versión de las guías.

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

        iv. Los activos sensibles que el TOE debe proteger.

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

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

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

        viii. La relación de librerías de terceros con sus correspondientes versiones utilizadas para implementar la funcionalidad de seguridad.

13. 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 configuración e instalación

    Debe ser posible identificar sin ambigüedad las guías y procedimientos de uso seguro y las guías de instalación y configuración que van a ser o han sido empleados en la evaluación del producto. Esto puede hacerse mediante la especificación de su versión, fecha de emisión, o cualquier

otro método que permita la identificación unívoca del documento como un resumen criptográfico del documento.

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 sean objeto de la evaluación, 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 la Declaración de Seguridad, en el Informe Técnico de Evaluación (ETR) y debe ser indicada en el informe de certificación.

Nota: En el caso de que el TOE se pueda ejecutar en diferentes plataformas el laboratorio debe garantizar que el TOE es el mismo, es decir, que el binario u objeto final sea el mismo, mediante, por ejemplo, la verificación del resumen criptográfico del TOE final. En el caso de que el binario sea diferente, se debe considerar como dos TOEs diferentes. En el caso de que el binario es el mismo, se deberá especificar en la Declaración de Seguridad la plataforma sobre la que se ha evaluado.

e) 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 sobre el entorno de ejecución el TOE puede no ser capaz de proporcionar todas las funcionalidades de seguridad o que posibles ataques pueden quedar fuera del alcance de la evaluación al quedar limitado el escenario de ataque por dichas hipótesis.

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.

f) Activos sensibles que deben de ser protegidos

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 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.

g) Descripción de las amenazas

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.

Por ejemplo, el hecho de que un usuario pueda inyectar información que modifique el comportamiento de una función de seguridad constituye una amenaza.

h) 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, es decir, el solicitante 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.

Nota: En el caso de que la Declaración de Seguridad declare cumplimiento con alguno de los anexos de requisitos funcionales de seguridad de la taxonomía de la CCN-STIC-140, no es suficiente con que el solicitante declare el cumplimiento con un determinado requisito, sino que debe describir a alto nivel, cómo el TOE implementa dicho requisito.

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.

El solicitante 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.

i) ***(MEC)*** La Declaración de Seguridad 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 de protocolo empleado y *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.

j) ***(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.

k) ***(MEB)*** La Declaración de Seguridad incluirá una descripción de los mecanismos de reconocimiento biométrico dentro del alcance de la evaluación biométrica y su finalidad. Esta descripción deberá detallar la modalidad biométrica, el tipo de sensor utilizado para la de captura de la muestra y el algoritmo biométrico. Además, se deberán detallar las funciones biométricas que han sido implementadas (reclutamiento, verificación y/o identificación) indicando las políticas específicas de las

mismas tales como el número de intentos de presentación permitidos y/o el máximo tiempo permitido para la captura de la muestra y los resultados que proporcionan cada una de estas funciones.

3.2 GUÍAS DE INSTALACIÓN, CONFIGURACIÓN Y OPERACIÓN DEL TOE

14. El solicitante debe proporcionar las guías o manuales relacionadas con la instalación, configuración y operación del producto de manera segura y que servirán como base para la evaluación.
15. En las **guías de instalación y configuración**, el solicitante debe describir los pasos necesarios para la instalación y configuración segura del producto. Esta documentación incluirá suficiente información para permitir realizar la instalación satisfactoriamente y poder establecer el producto en su configuración evaluada.
16. Adicionalmente, la guía de instalación deberá dar instrucciones para la identificación del TOE permitiendo a los usuarios verificar que el producto es conforme a la versión del TOE en la Declaración de Seguridad.
17. Si el producto permite varios modos de montaje/configuración (*set-up*), las guías deberán indicar claramente qué modo es el evaluado. La identificación de este modo deberá indicarse en la Declaración de Seguridad.
18. Si el producto admite diferentes parametrizaciones en su configuración, las guías deben diferenciar, sin lugar a dudas, entre las que forman parte del ámbito de la evaluación y las que no. Además, deberá indicarse el impacto en la seguridad de estas configuraciones. Esto implica la necesidad de revisar la documentación correspondiente a las distintas configuraciones del producto para su funcionamiento.
19. En las **guías de operación o procedimientos de empleo seguro**, el solicitante debe describir al menos:
    a) Cómo usar de manera segura el TOE.
    b) Cómo identificar unívocamente la versión del TOE evaluado.
    c) La funcionalidad accesible para cada rol de usuario.
    d) Los parámetros seguros configurables por el usuario a utilizar durante la operación del TOE.
20. 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 referencia 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.
21. 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 especificar todos los parámetros de seguridad que están bajo su responsabilidad.

Deberá detallar todos los sucesos relacionados con la seguridad cubiertos por las funciones de administración, así como pormenorizar 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.

22. Deberán señalarse 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.
23. 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.
24. 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

25. El solicitante proporcionará el entorno de pruebas del TOE al laboratorio. El entorno de pruebas deberá ser el mismo o equivalente al indicado en la Declaración de Seguridad y que permita probar la funcionalidad de seguridad descrita. En el caso de proporcionarse un entorno equivalente (no el mismo que el indicado en la Declaración de Seguridad), el solicitante deberá proporcionar una justificación demostrando que el entorno proporcionado es apropiado para la probar la funcionalidad de seguridad del producto, que será incluida en el Informe Técnico de Evaluación (ETR) remitido al Organismo de Certificación.
26. 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

27. El solicitante 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.
28. El autor de la Declaración de Seguridad detallará en la misma las funcionalidades de seguridad que serán evaluadas mediante el Módulo Código Fuente. Estas funcionalidades también serán detalladas en el informe de certificación.
29. Los certificados que empleen este módulo opcional serán identificados 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

30. El solicitante proporcionará la información de la implementación de los mecanismos criptográficos si el Módulo Criptográfico ha sido seleccionado como parte de la evaluación.
31. El autor de la Declaración de Seguridad detallará en la misma los algoritmos criptográficos que serán evaluados mediante el Módulo Criptográfico. Estos algoritmos también serán detallados en el informe de certificación.
32. 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.
33. 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 seguro de claves
    e) El mecanismo, formato y lugar de almacenamiento de claves.
    f) El mecanismo de transporte de claves.
34. 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.).

35. 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.
36. Adicionalmente a este documento, el evaluador debe disponer de acceso a dichos mecanismos criptográficos con la finalidad de comprobar la funcionalidad criptográfica.
37. Para cumplir este último requisito, podrá ser necesario que el solicitante proporcione herramientas específicas o versiones modificadas del producto que permitan el acceso directo a la funcionalidad criptográfica a través de una interfaz programable que permita al evaluador verificar su correcta implementación.
38. Los certificados que empleen este módulo opcional serán identificados como LINCE + MEC, de forma que se pueda identificar qué algoritmos han sido evaluados teniendo en cuenta su implementación.

3.6 *(MEB)* EVALUACIÓN BIOMÉTRICA

39. El solicitante proporcionará la información para interpretar los subsistemas que componen el sistema de reconocimiento biométrico implementado en el producto.
40. El autor de la Declaración de Seguridad detallará en la misma el método de reconocimiento biométrico y la modalidad a la que corresponde.
41. Para cada modalidad biométrica, el Organismo de Certificación proporcionará una instrucción técnica que establezca los criterios técnicos para la evaluación del TOE. La evaluación u homologación del algoritmo biométrico queda fuera del alcance de las certificaciones LINCE.
42. Los certificados que empleen este módulo opcional serán identificados como LINCE + MEB, de forma que se pueda determinar que la biometría ha sido evaluada teniendo en cuenta su implementación.

4. PROCEDIMIENTO DE EVALUACIÓN

43. 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.

44. La metodología está basada en gran parte en los niveles de menor garantía de [CC], por lo tanto, [CC] y [CEM] se pueden considerar documentos de apoyo a la metodología de evaluación para la Certificación Nacional Esencial de Seguridad (LINCE).

45. 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 el TOE puede ser identificado de manera unívoca.

1.3. Comprobar que la Declaración de Seguridad cumple estrictamente con todos los Requisitos Fundamentales de Seguridad de la taxonomía de productos declarada.

> **Nota**: La identificación de la taxonomía del producto según la guía CCN-STIC-140 es un requisito opcional en esta metodología que debe ser verificado por el laboratorio. 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, el solicitante deberá asignar a este campo el valor de NO APLICA.
>
> En todo caso, independientemente del cumplimiento estricto o no cumplimiento con los RFS definidos en los anexos de la guía CCN-STIC-140, la Declaración de Seguridad deberá contar con la aprobación de los requisitos en la declaración por parte de los responsables del CPSTIC y dicha aprobación deberá ser remitida al OC como evidencia en el ETR para la versión final evaluada de la Declaración de Seguridad.

1.4. Comprobar que se proporciona la identificación unívoca de las guías de operación o procedimientos de uso seguro y guías de configuración/instalación.

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

1.6. 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.

1.7. Comprobar que las funciones de seguridad, en su conjunto, mitigan o contrarrestan las amenazas descritas en la Declaración de Seguridad.

1.8. Comprobar que cada una de las funciones de seguridad está relacionada con una o varias de las amenazas incluidas en la Declaración de Seguridad.

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

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

1.11. Comprobar que se identifican las librerías de terceros que implementen funcionalidad de seguridad.

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

1.13. Indicar todas las no conformidades en relación con la Declaración de Seguridad.

4.2 ETAPA 2 – INSTALACIÓN DEL PRODUCTO Y ANÁLISIS DE LAS GUÍAS DE INSTALACIÓN, CONFIGURACIÓN Y OPERACIÓN

Tareas del evaluador

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

Nota: El solicitante 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 solicitante para esta tarea.

Nota: En el caso de que el solicitante proporcione una plataforma de pruebas equivalente (no la misma que la indicada en la Declaración de Seguridad), el evaluador deberá justificar en el informe de evaluación que el entorno proporcionado es apropiado para la probar la funcionalidad de seguridad del producto.

2.2. Comprobar que las guías de instalación y operación describen las funciones y privilegios para los diferentes roles de usuario definidos en el TOE que permitan instalar y operar el TOE de una manera segura.

2.3. 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 permite varios modos de montaje/configuración (*set-up*), las guías deberán indicar claramente qué modo es el evaluado. La identificación de este modo deberá estar indicado en la Declaración de Seguridad.
- Si el producto admite diferentes parametrizaciones en su configuración, las guías deben diferenciar, sin lugar a dudas, entre las que forman parte del ámbito de la evaluación y las que no.
- Si el producto requiere instalación, se instalará el producto en la configuración especificada en la guía de instalación. Adicionalmente el solicitante proporcionará la documentación relacionada con los distintos modos de configuración existentes en el producto.

2.4. Comprobar que la versión del TOE instalada se corresponde con la declarada en la Declaración de Seguridad y que la guías describen el procedimiento de identificación del TOE a los consumidores del mismo.

2.5. Describir la información relevante que permite que la instalación se desarrolle satisfactoriamente.

2.6. Describir todos los datos específicos de la configuración del sistema, cuando corresponda.

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

4.3 ETAPA 3 – 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 autor de la misma ha sido implementada en el producto.

Si las pruebas no son completas, el evaluador debe justificar la muestra realizada empleando como referencia el anexo A.2 de [CEM].

Para cada una de las pruebas realizadas, el evaluador deberá proporcionar la siguiente información:

a) La función de seguridad 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 pautas proporcionadas en [CEM] para la definición del plan de pruebas y realización de las pruebas independientes.

4.4 ETAPA 4 – ANÁLISIS DE VULNERABILIDADES

46. El propósito de esta etapa es determinar la existencia y valorar el esfuerzo necesario para explotar las deficiencias y debilidades del TOE en el entorno operacional. Para ello el evaluador deberá tener en cuenta la definición de la funcionalidad de seguridad del TOE, su entorno operacional y las hipótesis definidas en la Declaración de Seguridad.

Nota: El evaluador debe tomar como referencia las pautas proporcionadas en [CEM] para la realización de un análisis de vulnerabilidades.

Nota: Dada la limitación en tiempo y esfuerzo de la certificación, el evaluador podrá solicitar la realización de sesiones de trabajo con el solicitante 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 solicitante (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 teniendo en cuenta en dicho análisis la relación de librerías de terceros definidas en la Declaración de Seguridad por el solicitante.

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 dentro del potencial de ataque aplicable (ver párrafo 47) y documentar los posibles escenarios de ataque basados en dichas vulnerabilidades.

4.4.1. ANALÍSIS DE LA RESISTENCIA DE LOS MECANISMOS/FUNCIONES

47. Para cada uno de los escenarios de ataque diseñados por el evaluador, se realizará un estudio del nivel de recursos que un atacante necesitaría para explotar la vulnerabilidad asociada utilizando ese ataque, concepto que se define como "Potencial necesario para el ataque" o, simplemente, "Potencial de ataque".

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

Tareas del evaluador

5.4. Calcular el potencial de ataque para cada uno de los escenarios de ataque diseñados por el evaluador según el sistema de puntuación descrito en el apartado 4.4.1.1 Cálculo del Potencial de Ataque.

5.5. Indicar todas las no conformidades resultantes del análisis de vulnerabilidades.

4.4.1.1. CÁLCULO DEL POTENCIAL DE ATAQUE

49. 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.

Factor	Intervalo	Valor
Tiempo necesario	<= 1 día	**0**
	<= 1 semana	**1**
	<= 2 semanas	**2**
	<= 1 mes	**4**
	<= 2 meses	**7**
	<= 3 meses	**10**
	<= 4 meses	**13**
	<= 5 meses	**15**
	<= 6 meses	**17**
	> 6 meses	**19**
Experiencia del atacante	Inexperto	**0**

	Competente	**3**
	Experto	**6**
	Múltiples Expertos	**8**
Conocimiento necesario para el atacante	Información pública	**0**
	Información restringida	**3**
	Información sensible	**7**
	Información crítica	**11**
Acceso al producto por el atacante	Innecesario/Ilimitado	**0**
	Fácil	**1**
	Moderado	**4**
	Difícil	**10**
	No práctico	*****
Tipo de equipamiento necesario	Estándar	**0**
	Especializado	**4**
	Específico	**7**
	Múltiple Específico	**9**

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

Nota: * indica que el ataque es no explotable

50. El nivel de resistencia se computará teniendo en cuenta la suma de los valores asignados por el laboratorio para cada factor incluido en la Tabla 1. Además, debe tenerse en cuenta que el potencial de ataque debe ajustarse apropiadamente para aquellos escenarios de ataque que requieran la explotación previa de otra vulnerabilidad.

51. **Las vulnerabilidades con potencial de ataque mayor o igual a 19 se consideran residuales**. El resto de escenarios de ataque diseñados por el evaluador con un valor inferior a 19 deberán ser ejercitados en la ETAPA 5 – PRUEBAS DE PENETRACIÓN DEL TOE.

4.4.2. REVISIÓN DE CÓDIGO FUENTE *(MCF)*

52. 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. Se considerarán no conformidades las deficiencias que puedan derivar en una vulnerabilidad explotable en el TOE.

4.4.3. EVALUACIÓN CRIPTOGRÁFICA *(MEC)*

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

54. El evaluador debe disponer de soporte técnico por parte del solicitante 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 4.4.3.1.

  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 en base al estándar declarado.

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 fallo de conformidad con respecto a la implementación de referencia (en el caso de pruebas funcionales) o el estándar declarado (en el caso de análisis de código fuente).

4.4.3.1. VERIFICACIÓN DE LA IMPLEMENTACIÓN MEDIANTE PRUEBAS FUNCIONALES

55. 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.

56. A continuación, se puede observar en el siguiente ejemplo cómo se prueba un posible producto que implemente el algoritmo AES:

    a) “AES-CBC: existen cuatro pruebas posibles que deben ser superadas 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.

    b) 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.

    c) Test 1 – Para comprobar la 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.

d) 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.

e) 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.

f) 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.

57. Los resultados para cada prueba deben ser obtenidos por el evaluador con soporte del solicitante. El evaluador debe comparar los resultados con los de una implementación conocida de referencia autorizada por el Organismo de Certificación.

58. El CCN proporcionará las guías correspondientes para probar cada uno de los posibles algoritmos.

4.4.4. EVALUACIÓN BIOMÉTRICA (MEB)

59. La evaluación biométrica se realizará cuando el solicitante de la certificación haya seleccionado el Módulo Biométrico en su solicitud y haya identificado en la Declaración de Seguridad la funcionalidad biométrica objeto de evaluación mediante el Módulo Biométrico.

60. El evaluador debe disponer de soporte técnico por parte del solicitante para interpretar la información suministrada, así como información sobre los subsistemas que componen el sistema biométrico implementado en el producto.

Tareas del evaluador

MEB.1. Realizar las pruebas de evaluación biométrica en función de las pruebas definidas en las instrucciones técnicas para cada una de las modalidades biométricas admitidas en el CPSTIC.

El CCN proporcionará las instrucciones técnicas y guías que se deben seguir para realizar la evaluación de cada una de las modalidades biométricas. En estas guías se describirán las actividades de evaluación correspondientes a cada fase

MEB.2. Indicar todas las no conformidades en relación con cualquier debilidad o vulnerabilidad encontrada.

4.5 ETAPA 5 – PRUEBAS DE PENETRACIÓN DEL TOE

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

62. 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.

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

- Confirmar que los escenarios de ataque de las vulnerabilidades potenciales identificadas durante el análisis de vulnerabilidades son explotables.

64. 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. Además, se indicará a qué vulnerabilidad de las identificadas en la fase anterior se asocia esta prueba de penetración.

Para cada una de las pruebas realizadas, el evaluador deberá proporcionar la siguiente información:

a) La función o funciones de seguridad probadas
b) Vulnerabilidad asociada
c) Escenario de ataque
d) Objetivo de la prueba
e) El procedimiento con los pasos a seguir
f) Los resultados esperados y obtenidos
g) Conclusión y veredicto de la prueba

Ver sección 8 de [CCN-STIC-2004] para más información.

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

5. VEREDICTO DE LA EVALUACIÓN

65. 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 sustancial según lo establecido en esta metodología. En base a esta verificación y si todas las actividades de evaluación de la metodología han recibido el veredicto de PASA, el evaluador emitirá un veredicto positivo de la evaluación, proponiendo 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 sustancial, es decir que el TOE se caracteriza por no tener un nivel de resistencia medio, según lo establecido en esta metodología (ver apartado 4.4.1). 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. También se asignará el veredicto de FALLA si se supera el tiempo máximo de evaluación o las evidencias no cumplen los requisitos esperados. 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

66. 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. Esta planificación de recursos debe de ser acordada, de forma previa a la evaluación, entre el solicitante y el evaluador y contar con la autorización del Organismo de Certificación.

67. Una evaluación LINCE debe llevarse a cabo para una única versión del TOE con una carga de trabajo estimada de **25 jornadas laborables de una persona** con un periodo de realización máximo de **8 semanas**. Este tiempo incluye la redacción del Informe Técnico de Evaluación (ETR).

68. De acuerdo con esta limitación, es necesario tener en consideración que los evaluadores deben disponer de las capacidades y experiencia necesarias para llevar a cabo la evaluación del producto. El tiempo necesario para preparar a los evaluadores (Ej.- una tecnología nueva) no se debe tener en cuenta en la planificación de carga de trabajo.

69. Para los **módulos** opcionales (*MCF, MEC y MEB*), se añaden **5 jornadas** de esfuerzo y **2 semanas** de duración máxima adicionales para cada uno de los módulos. De este modo, se puede establecer una temporización modular.

70. Por ejemplo, para una evaluación que incluya los tres módulos, una evaluación LINCE debe llevarse a cabo con un esfuerzo de 40 jornadas laborables por una persona y con una duración máxima de 14 semanas.

71. 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 PERÍODO	ESFUERZO	DÍAS
ETAPA 1 – ANÁLISIS DE LA DECLARACIÓN DE SEGURIDAD	0	1	
ETAPA 2 – INSTALACIÓN DEL PRODUCTO Y ANÁLISIS DE LAS GUÍAS DE INSTALACIÓN, CONFIGURACIÓN Y OPERACIÓN	0	2	
ETAPA 3 – PRUEBAS FUNCIONALES	2	10	
ETAPA 4 – ANÁLISIS DE VULNERABILIDADES	11	17	
ANALÍSIS DE LA RESISTENCIA DE LOS MECANISMOS/FUNCIONES		2	
REVISIÓN DE CÓDIGO FUENTE (MCF)		2	
EVALUACIÓN CRIPTOGRÁFICA (MEC)		6	
EVALUACIÓN BIOMÉTRICA (MEB)		7	
ETAPA 5 – PRUEBAS DE PENETRACIÓN DEL TOE	30	10	
	TOTAL ESFUERZO	40	

7. RESULTADOS DE LA EVALUACIÓN

72. La evaluación de un producto de acuerdo con la metodología definida 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 sustancial. 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.

73. 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.

74. 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

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 por la que la información es accesible sólo para aquellos usuarios autorizados a tener acceso en el tiempo y la forma habilitada.

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 y el uso a los recursos e informaciones en el tiempo y la forma autorizada.

Documentación: información requerida para evaluar un objeto. Este documento puede ser relativo exclusivamente al producto o puede incluir referencias a otros productos con los que el objeto a evaluar se relaciona.

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: elementos ajenos al objeto a evaluar (Ej.- bases de datos, firewalls, etc.) necesarios para el correcto funcionamiento del TOE y los pasos a realizar para el correcto funcionamiento de los elementos del entorno.

Evaluación: valoración del grado de cumplimiento de un producto con los requisitos de evaluación definidos.

Evaluador: persona con suficientes habilidades, experiencia y formación académica acreditado para evaluar un producto.

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 a evaluar es trasladada al hardware y software. Ej.- código fuente

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

Laboratorio de evaluación: Entidad autorizada conforme a lo establecido en la orden PRE2740/2007 por el CCN y acreditada conforme a la norma ISO/IEC 17025 que se encarga de realizar la evaluación de seguridad del producto conforme a la metodología LINCE.

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

Objeto a evaluar (TOE): producto o partes de un producto que se someten a una evaluación de seguridad conforme a la configuración o configuraciones definidas en las guías de operación e instalación seguras referenciadas en su Declaración de Seguridad.

Operación: etapa de uso de un TOE.

Organismo de Certificación: entidad acreditada por la Entidad Nacional de Acreditación (ENAC) que expide certificaciones de seguridad TIC. En esta guía 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, autenticidad y/o trazabilidad.

Solicitante: entidad que solicita la evaluación. Usualmente, el patrocinador.

Test de penetración: pruebas llevadas a cabo por un evaluador en un TOE para confirmar si una vulnerabilidad identificada puede ser realmente explotada.

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

Vulnerabilidades: debilidad de alguna de las características de seguridad declaradas para 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
CEM	Common Criteria Evaluation Methodology
CNI	Centro Nacional de Inteligencia
ENS	Esquema Nacional de Seguridad
ETR	Evaluation Technical Report
LINCE	Certificación Nacional Esencial de Seguridad (LINCE)
MCF	Módulo Revisión de Código Fuente
MEB	Módulo de Evaluación Biométrica
MEC	Módulo de Evaluación Criptográfica
RD	Real Decreto
RFS	Requisitos Fundamentales de Seguridad
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