centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 2001

Definición de la Certificación Nacional Esencial de Seguridad (LINCE)

Octubre 2021

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

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.10.26 12:31:32 +02'00'

NIPO: 083-21-197-0

Fecha de Edición: Octubre 2021

CONTROL DE VERSIÓN

Versión	Comentario	Fecha
0.1	Versión en pruebas	Junio 2018
1.1	MEB	Octubre 2021

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.

Octubre de 2021

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1. OBJETO DEL DOCUMENTO

1. 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 medio. 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.
2. Este documento define la Certificación Nacional Esencial de Seguridad (LINCE) (LINCE) para un producto de seguridad de las tecnologías de la información y comunicaciones (TIC), incluyendo la definición de los actores involucrados en el proceso de evaluación, así como las distintas etapas del proceso de evaluación.
3. La evaluación y certificación de un producto de seguridad TIC es el único medio objetivo que permite valorar y acreditar la capacidad de un producto TIC para manejar información de forma segura. En España, esta responsabilidad está asignada al Centro Criptológico Nacional (CCN) a través del RD 421/2004 de 12 de marzo en su Artículo 1 y en su Artículo 2.1, el cual establece que el Director del CCN es la autoridad de certificación de la seguridad de las tecnologías de la información y la comunicación y autoridad de certificación criptológica en su ámbito.
4. En este sentido, el Centro Criptológico Nacional actúa como Organismo de Certificación (OC) del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI), de aplicación a productos y sistemas en su ámbito, tal y como marca la orden PRE/2740/2007, de 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.
5. Este esquema define la organización necesaria para que una evaluación de seguridad IT pueda llevarse a cabo por una tercera parte confiable y técnicamente capacitada, finalizando con la emisión de un certificado que demuestre que un producto o sistema cumple con los requisitos de seguridad especificados en su declaración de seguridad.
6. La certificación LINCE seguirá lo indicado en el procedimiento PO-005 (Certificación de productos) publicado en la web del CCN (https://oc.ccn.cni.es).
7. A lo largo de este documento, se indicarán las particularidades de la certificación LINCE, proporcionando información sobre la misma y poniendo en contexto a los posibles interesados.
8. Una evaluación STIC es un conjunto de pruebas que deberá realizar un laboratorio con el fin de verificar el cumplimiento de todos los Requisitos

Fundamentales de Seguridad (RFS). Estas pruebas consisten, entre otras, en un análisis de vulnerabilidades, pruebas de caja negra y pruebas en un entorno operacional. Para realizar una evaluación STIC se podrá emplear la metodología de evaluación [CCN-STIC-2002].

9. Para llevar a cabo una Certificación Nacional Esencial de Seguridad (LINCE), se ha definido una metodología de evaluación [CCN-STIC-2002] que puede ser también utilizada para realizar evaluaciones STIC tal y como se indica en las guías [CCN-STIC-106].

10. La Certificación Nacional Esencial de Seguridad (LINCE) certifica que un producto ha pasado exitosamente una evaluación de seguridad a través de una certificación autorizada por el CCN; la evaluación tiene las siguientes características principales:

    a) Debe de ser llevada a cabo en un tiempo y con una carga de trabajo acotada y predefinida.

    b) Debe analizar la conformidad del producto con sus requisitos fundamentales de seguridad conforme a lo definido en las guías [CCN-STIC-140].

    c) Debe medir la resistencia de las funciones de seguridad del producto.

    d) Debe de estar orientada al análisis de vulnerabilidades y test de penetración.

11. La Certificación Nacional Esencial de Seguridad (LINCE) está formada por un paquete base y tres (3) módulos opcionales que permiten incrementar las garantías de seguridad. Estos módulos opcionales son los siguientes:

    a) **Módulo de Evaluación Criptográfica (MEC)**: el objetivo de este módulo es evaluar funcionalmente los mecanismos criptográficos implementados en un producto. La inclusión de este módulo garantiza que las funciones criptográficas usadas han sido probadas funcionalmente. A lo largo del documento se empleará la convención *(MEC)*, para identificar los requisitos opcionales de este módulo.

    b) **Módulo de Revisión de Código Fuente (MCF)**: el objetivo de este módulo es incluir la revisión de código fuente del producto como parte de la evaluación. Esto permite evaluar el producto con mayor grado de profundidad al realizarse una evaluación de “Caja blanca”. A lo largo del documento se empleará la convención *(MCF)*, para identificar los requisitos opcionales de este módulo.

    c) **Módulo de Evaluación Biométrica (MEB)**: el objetivo de este módulo es evaluar la funcionalidad de reconocimiento biométrico implementada en un producto. La inclusión de este módulo garantiza que la biometría implementada en el producto ha sido probada funcionalmente. A lo largo del documento se empleará la convención *(MEB)*, para identificar los requisitos opcionales de este módulo.

12. Por lo tanto, se podrán realizar los siguientes tipos de evaluación como parte de la Certificación Nacional Esencial de Seguridad (LINCE):

    a) Básica: Evaluación LINCE

    b) Básica + MEC: Evaluación LINCE + Evaluación Criptográfica

    c) Básica + MCF: Evaluación LINCE + Revisión de Código fuente

    d) Básica + MEC + MCF: Evaluación LINCE + Evaluación Criptográfica + Revisión de Código Fuente

    e) Básica + MEB: Evaluación LINCE + Evaluación Biométrica

    f) Básica + MEB + MEC: Evaluación LINCE + Evaluación Biométrica + Evaluación Criptográfica

    g) Básica + MEB + MCF: Evaluación LINCE + Evaluación Biométrica + Revisión de Código Fuente

    h) Básica + MEB + MEC + MCF: Evaluación LINCE + Evaluación Biométrica + Evaluación Criptográfica + Revisión de Código Fuente

2. DEFINICIONES

13. **Laboratorio de evaluación LINCE:** Entidad acreditada conforme a lo establecido en la orden PRE2740/2007 por el CCN que se encarga de realizar la evaluación de seguridad del producto conforme a la metodología LINCE.
14. **Objeto a evaluar (TOE,** *Target of Evaluation***):** Objeto de la evaluación. Puede ser un producto completo o una parte del mismo. A lo largo del documento se emplearán indistintamente las palabra TOE y producto, siendo esta última referida al concepto de objeto de evaluación.
15. **Declaración de seguridad (ST,** *Security Target***):** Documento que describe las funciones de seguridad del producto que son objeto de evaluación.
16. **LINCE:** Certificación Nacional Esencial de Seguridad (LINCE).
17. **Desarrollador:** El término desarrollador indica la entidad que especifica, desarrolla, mantiene y/o fabrica el producto o alguno de sus componentes.
18. **Informe técnico de evaluación (ETR,** *Evaluation Technical Report***):** Informe emitido por el laboratorio de evaluación LINCE el cual resume los resultados de su evaluación.
19. **Informe de certificación:** Informe emitido por el Organismo de Certificación basado en el informe técnico de evaluación y que describe los elementos clave de la certificación realizada.
20. **Requisitos Fundamentales de Seguridad (RFS):** Descripción detallada de las características de seguridad que permiten mitigar las amenazas definidas en el problema de seguridad de la declaración de seguridad. Estos requisitos están especificados en las guías [CCN-STIC-140].
21. **Artefacto.** Objeto artificial o representación que presenta una copia de características biométricas o patrones biométricos sintéticos.
22. **Sujeto fidedigno.** Individuo legítimo dentro del sistema biométrico.
23. **Impostor:** Individuo que pretende suplantar a un sujeto fidedigno mediante el uso o no de artefactos.
24. **Atacante:** Individuo que ataca el sistema el cual puede ser un impostor, para ataques de presentación, o un usuario fidedigno, para ataques de ofuscación.
25. **Ataques de presentación (PAD):** La presentación de una muestra biométrica al subsistema de captura de datos biométricos con objeto de interferir con la operativa del sistema biométrico. Los ataques pueden ser de dos (2) tipos:
    a) De suplantación: en el que un atacante intenta ser reconocido como un sujeto fidedigno.
    b) De ofuscación: en el que un sujeto fidedigno pretende evadir ser reconocido como un individuo conocido por el sistema

26. **Detección de ataque de presentación (PAD).** Determinación automática de un ataque de presentación.
27. **Instrumento de ataque de presentación (PAI).** Característica biométrica u objeto utilizado en un ataque de presentación. Podrían ser artefactos, características biométricas sin vida, o características biométricas alteradas que se utilizan en un ataque.
28. **FNMR**. *False Non-Match Rate*. Falso negativo en la comparación. Esta tasa se define para algoritmos de comparación. En sistemas finales, donde la decisión se puede tomar tras varios intentos, suele denominarse **FRR** *False RejectionRate*
29. **FMR** *False Match Rate*: Falso positivo en la comparación. Esta tasa se define para algoritmos de comparación. En sistemas finales, donde la decisión se puede tomar tras varios intentos, suele denominarse **FAR** *False Acceptance Rate*.

3. ACTORES Y RESPONSABILIDADES EN LA CERTIFICACIÓN LINCE

3.1 LISTA DE ACTORES

30. Los siguientes actores están involucrados en el proceso de certificación:

    a) El patrocinador o el desarrollador es el encargado de la solicitud de evaluación del producto al Organismo de Certificación, de la financiación de la misma y es el encargado de diseñar, desarrollar y/o mantener el producto o sus componentes principales.

    b) El laboratorio de evaluación es una entidad acreditada por el Organismo de Certificación para desarrollar la evaluación del producto bajo este esquema.

    c) El Organismo de Certificación es el encargado de validar el informe procedente del laboratorio de evaluación y emitir el certificado en el caso de que la evaluación se supere satisfactoriamente.

3.2 PATROCINADOR O DESARROLLADOR

31. El desarrollador proporciona el producto, la documentación asociada al mismo y la declaración de seguridad.

32. Adicionalmente, se encarga de proporcionar el entorno de pruebas para la evaluación de seguridad del producto.

33. El desarrollador es también el encargado del desarrollo y es el responsable de proporcionar cualquier información que se precise y de dar asistencia técnica a los evaluadores si fuese necesario (entrenamiento, pruebas, suministro de una plataforma de evaluación).

34. *(MEC)* - Cuando las funciones de seguridad esenciales del producto contienen mecanismos criptográficos y se incluye el módulo de evaluación criptográfica como parte del proceso de certificación, el desarrollador también proporcionará la documentación que describe esos mecanismos.

35. *(MCF)* - Cuando el módulo de revisión de código fuente se incluya en el alcance de la evaluación, el desarrollador proporcionará el mismo al inicio de la evaluación.

36. *(MEB)* - Cuando las funciones de seguridad esenciales del producto contienen reconocimiento biométrico y se incluye el módulo de evaluación biométrico como parte del proceso de certificación, el desarrollador también proporcionará la documentación que describe esa funcionalidad.

37. El desarrollador tendrá adicionalmente las siguientes responsabilidades:

    a) Firmar un contrato con un laboratorio de evaluación acreditado por el CCN para llevar a cabo la evaluación de seguridad.

b) Realizar una petición de certificación al CCN usando el formulario de solicitud de certificación del producto [FOR-001].

c) Dar soporte al laboratorio de evaluación durante la evaluación para la realización de las pruebas.

Nota: En algunos casos, el desarrollador y el solicitante (*patrocinador*) de la certificación pueden ser entidades diferentes. Por simplicidad, se han listado como un único rol. En estos casos y en términos generales, el patrocinador será el encargado de financiar la evaluación y el desarrollador en dar el soporte técnico necesario para poder realizar el proceso de certificación.

3.3 LABORATORIO DE EVALUACIÓN

38. El laboratorio de evaluación es una entidad acreditada en el ENECSTI según lo definido en la orden PRE 2740/2007, de 19 de septiembre y en el procedimiento de Acreditación de Laboratorios [PO-006] para realizar evaluaciones de seguridad.

39. Con anterioridad a comenzar los trabajos de evaluación, deberá firmar un contrato con el desarrollador para evaluar un producto. En la negociación de dicho contrato el laboratorio tendrá la responsabilidad de valorar la declaración de seguridad presentada por el desarrollador y valorar la capacidad de evaluar el producto teniendo en cuenta las restricciones temporales y de carga de trabajo establecidas por la metodología de evaluación [CCN-STIC-2002], además de su cualificación técnica. Como respuesta a este análisis, el laboratorio elaborará un plan de evaluación que adjuntará a la solicitud de comienzo de evaluación en el que justificará la idoneidad de la declaración de seguridad y su propia capacitación técnica y propondrá las tareas de evaluación a realizar.

40. Se encarga de realizar la evaluación del producto de acuerdo con el procedimiento de certificación PO-005 y metodologías definidas para la evaluación [CCN-STIC-2002], así como de emitir el Informe Técnico de Evaluación (ETR) (ver plantilla en [CCN-STIC-2004]) al Organismo de Certificación para su correspondiente validación.

41. Las entidades de evaluación y su personal están obligados a mantener la confidencialidad sobre los productos que evalúan y los resultados que obtienen durante la evaluación.

42. La lista de entidades de evaluación acreditados por el CCN se encuentra actualizada en el sitio web del Organismo de Certificación.

3.4 ORGANISMO DE CERTIFICACIÓN

43. Las responsabilidades del Organismo de Certificación son las siguientes:

- Elaborar los criterios y la metodología de evaluación para la certificación. El Organismo de Certificación tiene la potestad para requerir el uso de métodos de evaluación específicos según las características del producto a evaluar.

- Especificar los procedimientos, formularios, guías y todo el resto de documentación necesaria para implementar la certificación LINCE, entre los cuales están:
    - El procedimiento de certificación de productos [PO-005].
    - El procedimiento de acreditación de laboratorios [PO-006].
    - La metodología de evaluación LINCE [CCN-STIC-2002].
    - La plantilla de declaración de seguridad LINCE [CCN-STIC-2003].
    - La plantilla para elaborar el informe técnico de evaluación [CCN-STIC-2004].
    - El formulario de Solicitud de Certificación de Producto [FOR-001].
    - El formulario de Solicitud de acreditación de laboratorio [FOR-005].
- Asegurar y verificar que los laboratorios satisfacen los criterios listados en el procedimiento de acreditación de laboratorios [PO-006].
- Revisar las solicitudes de certificación y evaluación y autorizar o denegar el inicio de la evaluación, teniendo en cuenta el plan de evaluación presentado por el laboratorio.
- Resolver las dudas existentes (Ej.- Interpretaciones de la metodología de evaluación a aplicar) durante el proceso de evaluación con el laboratorio en el caso de que fuera necesario.
- Validar técnicamente las tareas de evaluación documentadas en el ETR emitido por los laboratorios.
- Elaborar el informe de certificación y emitir el certificado correspondiente.
- Publicar, el producto certificado en la lista de productos certificados incluyendo la declaración de seguridad del producto y el informe de certificación.

4. FASES DEL PROCESO DE CERTIFICACIÓN

4.1 PREPARACIÓN DE LA CERTIFICACIÓN

44. Antes de formular una solicitud de certificación LINCE para un producto, el desarrollador debe:

    a) Preparar la declaración de seguridad del TOE siguiendo las guías establecidas en el documento Plantilla de la Declaración de Seguridad [CCN-STIC-2003]. La declaración de seguridad deberá incluir al menos los requisitos fundamentales de seguridad propios de la familia de productos a la que el TOE pertenece.

    b) Preparar la documentación necesaria para permitir a un usuario final utilizar el producto de manera segura (Guías de uso y de instalación del producto) y preparar el entorno para la realización de las pruebas de evaluación en colaboración con el laboratorio evaluador.

    c) *(MCF)* Si se ha incluido el Módulo de Evaluación de Código Fuente, el desarrollador debe preparar el código fuente para su entrega.

    d) *(MEC)* Si se ha incluido el Módulo de Evaluación Criptográfica, el desarrollador debe preparar la documentación que describe dichos mecanismos y preparar el entorno para la realización de las pruebas criptográficas.

    e) *(MEB)* – Si se ha incluido el Módulo de Evaluación Biométrica, el desarrollador debe preparar la documentación que describe la funcionalidad de reconocimiento biométrico y preparar el entorno para la realización de las pruebas biométricas.

Nota: si el producto no contempla alguna de las condiciones previas o si existe cualquier tipo de duda, el desarrollador debe contactar con el Organismo de Certificación para determinar si el producto puede ser evaluado bajo la certificación LINCE.

4.2 ELECCIÓN DE UN LABORATORIO DE EVALUACIÓN

45. El desarrollador debe firmar un acuerdo con el laboratorio de evaluación acreditado en el ENECSTI antes de enviar la solicitud de certificación del producto.

46. Tanto el desarrollador como el laboratorio deben acordar el alcance de la evaluación atendiendo a la declaración de seguridad presentada por el solicitante. El laboratorio será el encargado de analizar la declaración de seguridad para verificar que es posible evaluar todos los mecanismos de seguridad incluidos teniendo en cuenta las restricciones temporales y de carga de trabajo fijadas en la metodología [CCN-STIC-2002].

4.3 SOLICITUD DE CERTIFICACIÓN

47. El desarrollador elaborará y enviará al Organismo de Certificación:

    a) La solicitud de certificación del producto (véase [FOR-001]).

    b) La declaración de seguridad del producto (véase la plantilla [CCN-STIC-2003]).

> **Nota:** En caso de ser necesario, el desarrollador podrá entregar un documento anexo explicando cualquier particularidad relacionada con el proceso de certificación.

4.4 SOLICITUD DE EVALUACIÓN

48. El laboratorio elaborará y enviará al Organismo de Certificación una solicitud de evaluación que incluya:

    a) Una justificación de la idoneidad de la declaración de seguridad para realizar una evaluación LINCE, dadas las restricciones de carga de trabajo impuestas por la metodología.

    b) Un plan de evaluación en el que muestre la planificación de las tareas de evaluación a realizar.

    c) Una justificación de la capacitación técnica e imparcialidad del laboratorio y evaluadores para llevar a cabo la evaluación en función de la declaración de seguridad.

4.5 ANÁLISIS DE LAS SOLICITUDES

49. El Organismo de Certificación analiza las solicitudes de certificación y evaluación y la declaración de seguridad del producto.

50. Existen varias razones para que una solicitud de certificación sea rechazada, en particular:

    a) Solicitud incompleta.

    b) Declaración de seguridad incompleta.

    c) La declaración de seguridad resulta confusa, es decir, la declaración de seguridad no incluye los requisitos fundamentales de seguridad propios de la familia de productos a la que pertenece. Por ejemplo, el producto es un cortafuegos y la única función de seguridad incluida en el alcance de la certificación es la autenticación del usuario para modificar la configuración de su producto.

    d) Las características del producto no permiten realizar una evaluación LINCE de manera apropiada, dadas las limitaciones en tiempo que tiene esta certificación.

    e) Fallo al respetar los pre-requisitos identificados en la sección 4.3 o 4.4.

51. Después de que se acepte la solicitud de certificación por el Organismo de Certificación, el proyecto de certificación se registra y se informa a los actores (desarrollador y laboratorio de evaluación) sobre la aceptación del inicio del proyecto.
52. Si el OC lo considerará necesario, podría organizar una reunión de comienzo de evaluación con el laboratorio para definir la aproximación a seguir por el laboratorio durante la evaluación.
53. Tras el análisis realizado, si el Organismo de Certificación lo considera necesario, proporcionará guías o documentos de apoyo de uso obligatorio u opcional, dependiendo del caso, para la realización de la evaluación. El OC podrá realizar recomendaciones para el desarrollo de la evaluación, así como fijar metodologías de evaluación adicionales a seguir por parte del laboratorio.
54. El momento de la notificación de la autorización de comienzo de evaluación se considera la fecha de inicio de la evaluación.

4.6 EJECUCIÓN DE LA EVALUACIÓN

4.6.1. INFORMACIÓN GENERAL SOBRE EL PROCEDIMIENTO DE EVALUACIÓN

55. La evaluación debe ser ejecutada por un laboratorio acreditado en el ENECSTI siguiendo la metodología de evaluación (véase [CCN-STIC-2002]) para garantizar que la certificación LINCE cumple la finalidad para la que fue diseñada, así como para asegurar la homogeneidad de los resultados entre los distintos laboratorios.
56. Existe la posibilidad de que el Organismo de Certificación defina para ciertos tipos de productos una metodología de evaluación complementaria y específica asociada. En este caso, el laboratorio será notificado y la metodología propuesta deberá ser utilizada por el laboratorio de evaluación.
57. Si el tiempo programado para la evaluación se excede, el Organismo de Certificación puede decidir cerrar el expediente de certificación, con independencia de las obligaciones contractuales que pudieran existir entre desarrollador y laboratorio.
58. La metodología incluye las siguientes actividades:
    a) Análisis de la conformidad: El evaluador debe verificar la conformidad del producto con respecto a la declaración de seguridad y documentación asociada.
    b) Análisis de vulnerabilidades y test de penetración: El evaluador debe realizar un análisis de vulnerabilidades del producto y ejecutar los test de penetración diseñados, considerando el estado el estado del arte de amenazas y vulnerabilidades públicamente disponibles, para verificar la efectividad de las funciones de seguridad del TOE.
59. Las fases de evaluación son las siguientes:
    a) Análisis de la declaración de seguridad.

b) Instalación del producto.

c) Análisis de conformidad – análisis de la documentación.

d) Análisis de conformidad – pruebas funcionales.

e) Análisis de vulnerabilidades.

i. Análisis de la resistencia de los mecanismos/funciones

ii. *(MCF)* Revisión del código fuente.

iii. *(MEC)* Evaluación criptográfica.

iv. (MEB) Evaluación Biométrica

f) Test de penetración del TOE.

60. Los resultados se presentan en un informe técnico de evaluación (ETR) que se envía al Organismo de Certificación para su validación técnica.

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

62. Además, el desarrollador deberá de proporcionar el entorno operativo y de pruebas antes de comenzar la evaluación, así como dar soporte al evaluador durante la instalación del TOE.

4.6.2. RESTRICCIONES TEMPORALES Y DE ESFUERZO DE LA EVALUACIÓN

63. 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.

64. 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**.

65. 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.

66. Para los **módulos** opcionales (*Módulo Código Fuente, Módulo Criptográfico y Módulo Biométrico*), se añaden **5 jornadas** de esfuerzo y **2 semanas** de duración máxima adicionales para cada uno de los módulos.

67. Incluyendo los tres (3) 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. Para una información más detallada, véase [CCN-STIC-2002].

4.7 FASE DE CERTIFICACIÓN

68. Cuando la evaluación se completa, el evaluador enviará el Informe Técnico de Evaluación (ETR) al Organismo de Certificación del CCN. A grandes rasgos el proceso de certificación se compone de los siguientes pasos:

    a) Análisis técnico y validación del ETR. La fase de validación del ETR podrá realizarse mediante el estudio y análisis del ETR y/o sesiones de análisis a las que pueden ser convocados los evaluadores del producto para ganar más conocimiento sobre los trabajos realizados. En caso del que el Organismo de Certificación lo considere oportuno a raíz de dicho análisis, se podrá requerir más información o incluso trabajo adicional al laboratorio de evaluación si la información o trabajo se considera insuficiente.

    b) Elaboración de un informe de certificación, cuyo contenido se detalla en la sección 4.7.1.

    c) Seguimiento de los pasos para la emisión del certificado tal y como marca la Orden PRE/2740/2007 y desarrollado en el procedimiento de Certificación de productos [PO-005].

4.7.1. INFORME DE CERTIFICACIÓN

69. El informe de certificación es un documento dirigido a potenciales usuarios del producto evaluado (TOE) y cuyo objetivo es proporcionar información sobre las características de seguridad que han sido sometidas a evaluación y las condiciones de instalación, configuración y uso seguro y debe de contener los siguientes puntos:

    a) Una introducción describiendo el objeto de la evaluación.

    b) Una visión general del producto, realizando una descripción del mismo, versión e identificación unívoca del objeto de evaluación y listado de las funciones de seguridad y la configuración del producto evaluado.

    c) El objetivo y limitaciones de la evaluación.

    d) Una descripción de los riesgos residuales del producto cuando se utiliza según la configuración evaluada

    e) Guías para la administración y configuración segura del producto incluyendo entrega, preparación del entorno, instalación y configuración del TOE.

    f) Instrucciones para un uso seguro del producto.

    g) El resultado de la evaluación

4.8 VALIDEZ DEL CERTIFICADO

70. Un certificado LINCE se emite indicando la versión específica del producto que fue evaluada. Si este producto evoluciona, sus nuevas versiones no serán certificadas por defecto. El proceso de "*Assurance Continuity*" o continuidad de la garantía [AC] se usa para facilitar el mantenimiento del certificado en versiones nuevas del producto. Este proceso es aplicable a la certificación LINCE.

71. Se recomienda revisar la validez del certificado a los veinticuatro meses desde su emisión. En todo momento el desarrollador podrá optar al proceso de renovación del certificado o re-certificación del mismo, según lo establecido en el procedimiento de certificación PO-005.

5. PUBLICIDAD

72. El desarrollador puede publicitar la certificación LINCE del producto. Debe hacerlo de forma honesta y entendible para el usuario final, de acuerdo a lo especificado en la orden PRE/2740/2007. En términos generales, deberán indicar:

    a) La referencia del certificado.

    b) La fecha de certificación del producto.

    c) Las referencias y versión del producto certificado.

    d) Referencias a la declaración de seguridad e informe de certificación del producto.

73. El Organismo de Certificación se reserva la posibilidad de vigilar cualquier uso abusivo del certificado LINCE de acuerdo a lo establecido en los artículos 149 y 152 de la Orden PRE/2007/2740.

6. REFERENCIAS

[AC]	Assurance Continuity: CCRA Requirements. Version 2.1
[CC]	Common Criteria for Information Technology Security Evaluation.
[CCN-STIC-2002]	Metodología de Evaluación para 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-106]	Procedimiento de inclusión de productos de seguridad TIC cualificados en el CPSTIC.
[CCN-STIC-140]	Taxonomía de referencia para productos de Seguridad TIC
[FOR-001]	Solicitud de Certificación de Producto
[FOR-005]	Solicitud de acreditación de laboratorio
[PO-005]	PO-005 Certificación de productos.
[PO-006]	PO-006 Acreditación de laboratorios.

7. ACRÓNIMOS

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
ENECSTI	Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de Información
ENS	Esquema Nacional de Seguridad
ETR	Evaluation Technical Report – Informe Técnico de Evaluación
LINCE	Certificación Nacional Esencial de Seguridad (LINCE)
MCF	Módulo Código Fuente
MEB	Módulo de Evaluación Biométrica
MEC	Módulo de Evaluación Criptográfica
OC	Organismos de Certificación
RD	Real Decreto
RFS	Requisitos Fundamentales de Seguridad
ST	Security Target- Declaración de Seguridad
STIC	Seguridad de las Tecnologías de la Información y Comunicación

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