centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 2001

Definición de 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 11:36:12 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-087-5

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. 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.
2. Este documento define la Certificación Nacional Esencial de Seguridad (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 de un producto de seguridad TIC es el único medio objetivo que permite valorar y certificar la capacidad de un producto TIC para manejar información con el nivel de seguridad manifestado por el fabricante en su declaración de seguridad. 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 TIC 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). Para la certificación del Módulo de Evaluación Biométrica, se seguirá adicionalmente lo indicado en el procedimiento PO-008 (Certificación de productos en dominios técnicos).

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. Para llevar a cabo una Certificación Nacional Esencial de Seguridad (LINCE), se ha definido la metodología de evaluación [CCN-STIC-2002] que deberá ser empleada en los procesos de certificación LINCE asociados a la cualificación de productos definida en la guía [CCN-STIC-106].

9. 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 habiendo sido evaluado por uno de los laboratorios autorizados al efecto en el ENECSTI; la evaluación LINCE 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 los requisitos fundamentales de seguridad definidos y aprobados por los responsables del Catálogo de Productos de Seguridad TIC (CPSTIC) del Departamento de Productos y Tecnologías del CCN(CCN-PYTEC).

    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.

10. 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.

11. 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. ACTORES Y RESPONSABILIDADES EN LA CERTIFICACIÓN LINCE

2.1 LISTA DE ACTORES

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

    a) El solicitante es el encargado de la solicitud de evaluación del producto al Organismo de Certificación, y de la financiación de la misma.

    b) El desarrollador es el encargado de diseñar, desarrollar y/o mantener el producto o sus componentes principales. Dependiendo de la naturaleza del producto, así como de su ciclo de vida, puede tenerse en consideración un actor adicional que sería el fabricante, el cual suele desempeñar labores relacionadas con hardware.

    c) El laboratorio de evaluación es una entidad acreditada conforme a la norma ISO/IEC 17025 y autorizada por el Organismo de Certificación para desarrollar la evaluación del producto bajo el ENECSTI.

    d) 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.

2.2 SOLICITANTE Y/O DESARROLLADOR

13. El solicitante y/o el desarrollador proporcionan el producto, la documentación asociada al mismo y la declaración de seguridad. Adicionalmente, se encarga de proporcionar el entorno de pruebas para la evaluación de seguridad del producto.

14. El desarrollador es 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, corrección de los informes de observación (OR) del laboratorio). En caso de que en la evaluación sólo participe el solicitante, las actividades anteriores recaerán sobre esta entidad.

15. *(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.

16. *(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.

17. *(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.

18. El solicitante tendrá, adicionalmente, las siguientes responsabilidades:

a) Firmar un contrato con un laboratorio de evaluación autorizado 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 de la certificación pueden ser entidades diferentes. Por simplicidad, se han listado como un único rol. En estos casos y en términos generales, el solicitante será el encargado de financiar la evaluación y el desarrollador en dar el soporte técnico necesario para poder realizar el proceso de certificación.

2.3 LABORATORIO DE EVALUACIÓN

19. El laboratorio de evaluación es una entidad acreditada conforme a la norma ISO/IEC 17025 y autorizada 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.

20. Con anterioridad al comienzo de los trabajos de evaluación, deberá firmar un contrato con el solicitante 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 en base a las restricciones temporales establecidas por la metodología y su propia capacitación técnica y propondrá las tareas de evaluación a realizar.

21. Se encarga de realizar la evaluación del producto de acuerdo con el procedimiento de certificación [PO-005] ([PO-008] si se emplea el módulo MEB) y metodología definida 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.

22. 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.

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

2.4 ORGANISMO DE CERTIFICACIÓN

24. 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].
    - El procedimiento de certificación de productos en dominios técnicos [PO-008].
    - 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 posibles dudas que puedan aparecer durante el proceso de evaluación, como por ejemplo, las relacionadas con la interpretación de la metodología de evaluación a aplicar.
- 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.

3. RELACIÓN ENTRE EL PROCESO DE CUALIFICACIÓN Y LA CERTIFICACIÓN LINCE

25. La metodología LINCE será empleada exclusivamente para la cualificación de productos para el CPSTIC (Catálogo de Productos de Seguridad TIC) mantenido por el Departamento de Productos y Tecnologías del CCN (CCN-PYTEC), conforme a lo establecido en la guía [CCN-STIC-106].

26. Teniendo en cuenta lo anterior, para que el Organismo de Certificación del CCN (OC) tramite una certificación LINCE, será necesario que el solicitante previamente haya solicitado la cualificación del producto para su inclusión en el CPSTIC (Catálogo de Productos de Seguridad TIC).

27. Como parte de la valoración de la idoneidad de un producto para su inclusión en el catálogo CPSTIC, los responsables del CPSTIC deben verificar el cumplimiento de las características de seguridad especificadas en la declaración de seguridad del producto candidato contra los requisitos marcados para la familia de productos, por lo que será necesaria la revisión de la declaración de seguridad del producto para su inclusión en el CPSTIC por parte de los responsables del CPSTIC.

28. Por lo tanto, el procedimiento de certificación del producto contra la metodología LINCE, sólo podrá comenzarse si los responsables del CPSTIC requieren una certificación LINCE al solicitante y éste cuenta con el visto bueno de la declaración de seguridad por parte del CPSTIC.

29. Si en el transcurso de la evaluación el solicitante quisiera modificar la declaración de seguridad, esta modificación deberá ser autorizada previamente por los responsables del CPSTIC antes de que sea considerada por el laboratorio como evidencia de evaluación.

30. El procedimiento de cualificación y certificación LINCE se resume en el siguiente gráfico:

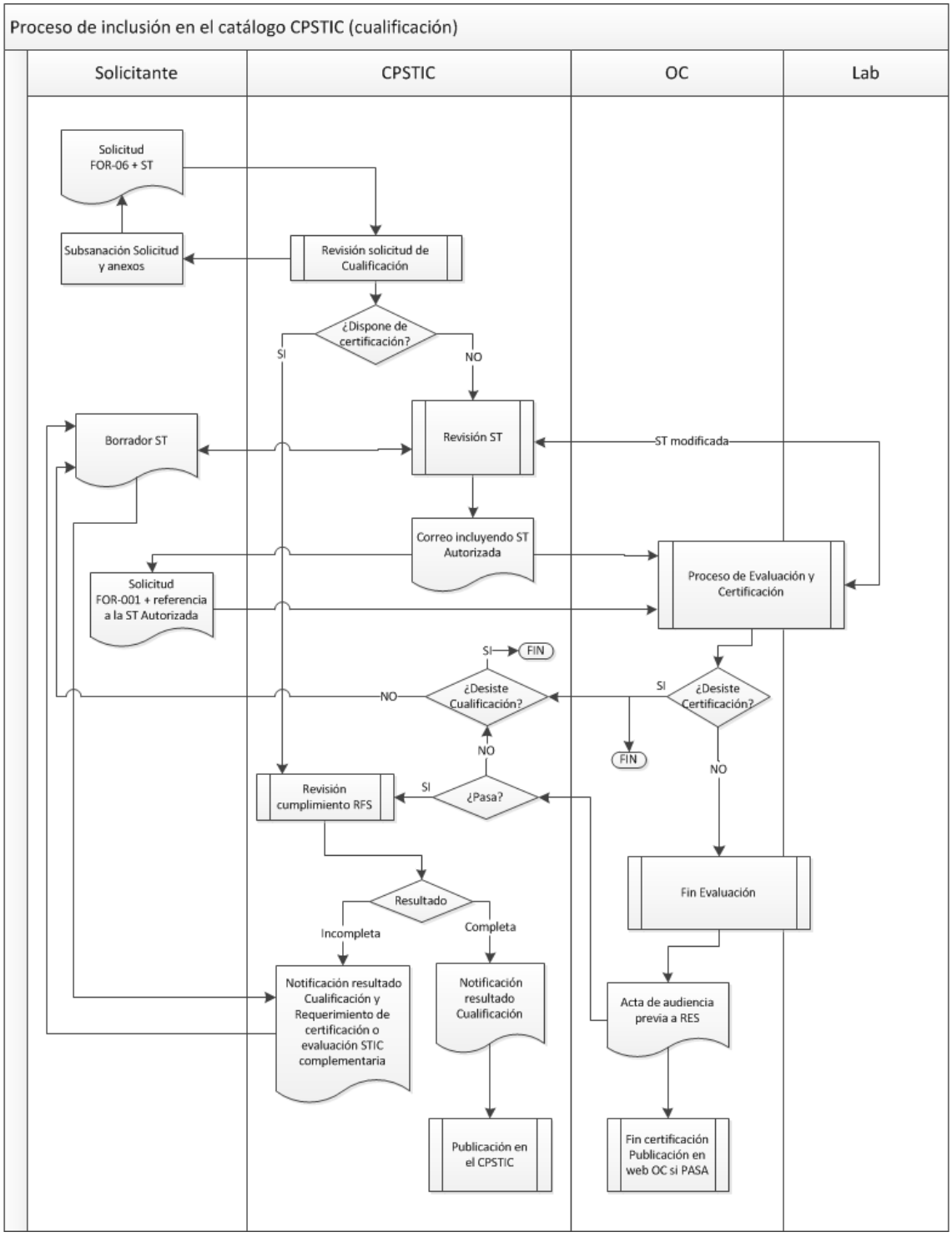

Ilustración 1 - Procedimiento de cualificación y certificación

4. FASES DEL PROCESO DE CERTIFICACIÓN

4.1 PREPARACIÓN DE LA CERTIFICACIÓN

31. Antes de formular una solicitud de certificación LINCE para un producto, el solicitante debe:

    a) Solicitar la cualificación siguiendo los procedimientos marcados por la guía [CCN-STIC-106], mediante la remisión del formulario FOR-006 y una declaración de seguridad aprobada por los responsables del CPSTIC conforme a los requisitos marcados en la guía [CCN-STIC-140].

    b) 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.

    c) 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.

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

    e) *(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.

    f) *(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.

4.2 ELECCIÓN DE UN LABORATORIO DE EVALUACIÓN

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

33. Tanto el solicitante como el laboratorio deben acordar el alcance de la evaluación atendiendo a la declaración de seguridad presentada, previa aprobación de dicha declaración de seguridad por los responsables del CPSTIC. El laboratorio será el encargado de analizar la declaración de seguridad para verificar que es posible evaluar todos los mecanismos de seguridad aprobados, teniendo en cuenta las restricciones temporales y de carga de trabajo fijadas en la metodología [CCN-STIC-2002]. En caso contrario, se lo comunicará al solicitante y a los responsables del CPSTIC para que revisen los requisitos marcados dentro de la declaración de seguridad.

4.3 SOLICITUD DE CERTIFICACIÓN

34. El solicitante 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]). La declaración de seguridad referenciada en la solicitud de certificación deberá ser la misma que haya aprobado los responsables del CPSTIC y que habrá remitido al Organismo de Certificación.

    c) El informe de aprobación de la declaración de seguridad emitido por los responsables del CPSTIC.

4.4 SOLICITUD DE EVALUACIÓN

35. 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

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

37. Existen varias razones para que una solicitud de certificación sea rechazada o sea solicitada su subsanación, en particular:

    a) Solicitud incompleta.

    b) Declaración de seguridad incompleta.

    c) No incluir el informe de aprobación de la declaración de seguridad emitido por los responsables del CPSTIC para la versión de la declaración de seguridad presentada en la solicitud.

    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 ó 4.4.

38. 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 participantes (solicitante y laboratorio de evaluación) sobre la aceptación del inicio del proyecto.

39. 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. En todo caso, el OC informará al laboratorio sobre la obligatoriedad de notificar las posibles modificaciones sobre la declaración de seguridad aprobada por los responsables del CPSTIC. En el caso de que se produzcan modificaciones en esta evidencia, el laboratorio informará al OC de este hecho y a los responsables del CPSTIC para que procedan a analizar la nueva declaración de seguridad y en su caso procedan a su autorización. El laboratorio no deberá tener en cuenta la declaración de seguridad modificada en la evaluación hasta que se notifique la autorización de la versión por parte de los responsables del CPSTIC.

40. Tras el análisis realizado, si el Organismo de Certificación lo considera necesario, proporcionará instrucciones técnicas 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.

41. 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

42. La evaluación debe ser ejecutada por un laboratorio autorizado 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.

43. 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.

44. Adicionalmente el Organismo de Certificación, dependiendo de las familias de productos incluidas en el CPSTIC, podrá definir nuevos dominios técnicos de certificación dentro de su procedimiento operativo PO-008, para lo que contará con el apoyo de expertos técnicos en la tecnología específica objeto de certificación.

45. 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 el solicitante y el laboratorio.

46. 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.

47. Las fases de evaluación son las siguientes:

    a) Análisis de conformidad - Análisis de la declaración de seguridad.

    b) Análisis de conformidad- Instalación del producto y análisis de las guías de operación e instalación.

    c) Análisis de conformidad - Pruebas funcionales.

    d) Análisis de vulnerabilidades.

        i. Análisis de la resistencia de los mecanismos/funciones de seguridad.

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

        iii. *(MEC)* Evaluación criptográfica.

        iv. (MEB) Evaluación Biométrica

    e) Pruebas de penetración del TOE.

48. Los resultados se presentarán en un informe técnico de evaluación (ETR) que se enviará al Organismo de Certificación para su validación técnica.

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

50. 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

51. 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.

52. 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**.

53. 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.

54. 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.

55. 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].

4.6.3. EMISIÓN Y TRATAMIENTO DE INFORMES DE OBSERVACIÓN (ORs)

56. Teniendo en cuenta las restricciones temporales y de esfuerzo definidas, se debe establecer un procedimiento para la gestión de la emisión y tratamiento de los Informes de Observación (ORs)[1] emitidos por los laboratorios.

57. El procedimiento de gestión de ORs en las certificaciones LINCE, debe tener en cuenta las restricciones de carga de trabajo del laboratorio y el plazo temporal máximo establecido en la metodología, por lo tanto, el tratamiento de las ORs por el solicitante no debe interferir con estos requisitos de la metodología.

58. Teniendo en cuenta lo anterior, el laboratorio no admitirá el tratamiento de las ORs por el solicitante, salvo que se dé una situación en que la observación pueda ser solventada en un plazo de tiempo que no afecte a la carga de trabajo máxima planificada y al tiempo máximo de evaluación fijado. Se recuerda que el solicitante puede solicitar al Organismo de Certificación el desistimiento de la evaluación en cualquier momento al ser un procedimiento administrativo común.

59. En el caso en el que el laboratorio deba emitir una OR, lo hará siempre informando a la vez al solicitante y al Organismo de Certificación (OC). Se espera que el laboratorio acuerde con el solicitante los plazos para el tratamiento de la OR, siempre teniendo en cuenta la carga de trabajo y plazos máximos de la certificación LINCE.

60. Se espera que el laboratorio suspenda las actividades de evaluación que se vean afectadas por la OR que va a ser tratada por el solicitante, de forma que no se consuman recursos de manera innecesaria hasta que no se reciba la propuesta de tratamiento de la OR por parte del solicitante. Así mismo, el laboratorio debe estar dispuesto a ajustar su planificación conforme a los límites máximos establecidos intentando proporcionar el tiempo necesario para poder solventar el mayor número de ORs durante el período máximo de evaluación.

61. En todo caso, la valoración de la consideración del tratamiento de la OR será realizada por el laboratorio conforme a su plan de evaluación y consensuada con

[1] El laboratorio emitirá un Informe de Observación (OR) si durante los trabajos de evaluación detecta que el TOE no cumple alguno de los requisitos fijados en la metodología de evaluación.

el OC. El laboratorio justificará al OC que la posible solución no afecta al plazo máximo de evaluación o carga planificada, por lo que junto la descripción del tratamiento de la OR deberá enviar una justificación del plazo de resolución previsto por el solicitante y una re-planificación de la evaluación que tenga en cuenta el impacto a la evaluación del tratamiento de la OR por parte del solicitante.

62. A modo de resumen, aunque la planificación de la evaluación sea menor al tiempo máximo de la evaluación (8 semanas), en caso de aparecer ORs, el solicitante podría dilatar el tiempo total al máximo marcado por la metodología de evaluación (8 semanas más 2 semanas por módulo opcional declarado) con el fin de poder disponer de tiempo extra para solventar estas ORs. Todo esto, teniendo en cuenta el esfuerzo previo realizado por el laboratorio, la planificación de las ORs y el esfuerzo total limitado a realizar por el laboratorio (25 jornadas + 5 jornadas por módulo opcional declarado en la ST).

4.7 FASE DE CERTIFICACIÓN

63. Cuando la evaluación se complete, 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. Si el resultado del análisis así lo aconseja, el Organismo de Certificación podrá solicitar al laboratorio el envío de información adicional o la realización de trabajos adicionales; esta solicitud se realizará mediante las correspondientes no conformidades/observaciones que deberán ser resueltas por el laboratorio.

    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. TRATAMIENTO DE NO CONFORMIDADES Y PLAZO MÁXIMO DE LA FASE DE EVALUACIÓN

64. Si como consecuencia de la validación del informe técnico de evaluación por parte del Organismo de Certificación, se detecta alguna desviación en el cumplimiento de la norma por parte del laboratorio que impactase al TOE o evidencias de evaluación responsabilidad del solicitante, el laboratorio deberá emitir la OR correspondiente y realizar su tratamiento de forma adecuada dentro del proceso de evaluación.

65. El esfuerzo correspondiente a este caso no será computado como parte del esfuerzo de la evaluación y el laboratorio deberá realizar el esfuerzo necesario para solventar la no conformidad u observación emitida por el Organismo de Certificación, siempre teniendo en cuenta que el plazo máximo para la entrega de la versión corregida del nuevo informe técnico de evaluación no debe superar 30 días naturales desde la fecha de validación, de forma que si no se cumple este plazo se convocará la reunión de audiencia previa a la resolución, y el laboratorio deberá tratar las desviaciones detectadas dentro de su plan de calidad y serán objeto de revisión en las auditorías de seguimiento de la acreditación.

66. La duración máxima de la fase de evaluación de un expediente vendrá fijada por la suma de:

    - Ocho (8) semanas (más dos semanas por módulo opcional declarado)
    - Cuatro (4) semanas para la validación por el OC del ETR entregado por el laboratorio
    - Treinta (30) días naturales (en caso de que el laboratorio deba emitir una versión corregida del ETR)

67. Por tanto, la duración máxima será de dieciséis (16) semanas (más las semanas asociadas a la inclusión de módulos adicionales).

4.7.2. INFORME DE CERTIFICACIÓN

68. 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 PROCEDIMIENTO PARA AUTORIZACIÓN DE RE-EVALUACIÓN DE UN PRODUCTO

69. De acuerdo con la metodología LINCE, el laboratorio deberá asignar el veredicto FALLA a la evaluación si se verifica que, una vez finalizado el plazo máximo de evaluación, el TOE no cumple con los requisitos fijados en la Declaración de Seguridad; en este caso, el Organismo de Certificación Procederá a la resolución desestimatoria del expediente de certificación. .

70. El ENECSTI es sensible a los esfuerzos que suponen los procesos de certificación por parte de los solicitantes, por lo que considera necesario establecer un procedimiento de re-utilización de los resultados de las actividades de evaluación de procesos de certificación que han resultado desestimados.

71. El proceso de re-evaluación de un producto es de aplicación a aquellos productos que, habiendo pasado un primer proceso de certificación LINCE, han resultado desestimados después de la reunión de audiencia previa y siempre y cuando no hayan transcurrido más de seis meses desde la reunión de audiencia previa a la resolución.

72. En estos casos, el Organismo de Certificación podrá iniciar, conforme al procedimiento PO-005, un nuevo expediente de certificación en el que se autorice al laboratorio encargado de la evaluación inicial a reutilizar los resultados de la misma. El esfuerzo asignado a este nuevo expediente puede ser inferior al fijado con carácter general y será establecido de acuerdo con los cambios introducidos por el fabricante en el TOE.

73. La reevaluación del TOE y/o la reutilización de resultados de la evaluación sólo será posible si se produjo el final formal del expediente inicial, esto es, si el Organismo de Certificación emitió la convocatoria de la reunión de audiencia previa a la resolución, informando al solicitante sobre el resultado de la evaluación y del sentido de la resolución del expediente de certificación.

74. El proceso de re-evaluación LINCE comenzará con el proceso habitual de solicitud de certificación LINCE, en el que se añade la entrega de una evidencia adicional que se denomina Informe de Análisis de Impacto. En este informe el solicitante debe informar al Organismo de Certificación sobre los cambios introducidos en el TOE con respecto al TOE empleado en la certificación original desestimada. Se espera que este informe sea lo suficientemente detallado, de forma que tanto el Organismo de Certificación como el laboratorio evaluador, puedan estimar los esfuerzos necesarios para realizar la nueva evaluación y puedan estimar el nivel de pruebas de regresión que se deben ejecutar en el transcurso de la nueva evaluación. El contenido mínimo necesario de este informe será:

    a) Identificación del TOE

    b) Referencia al expediente de certificación original.

    c) Descripción general de los cambios

    d) Listado de evidencias del solicitante afectadas por los cambios

e) Descripción de los cambios introducidos en las evidencias

f) Conclusiones y estimación del impacto

75. Una vez que se analicen los cambios, el OC los tendrá en cuenta para analizar el nuevo plan de evaluación que remita el laboratorio en la solicitud de comienzo de evaluación conforme al [PO-005]. En este nuevo plan de evaluación el laboratorio deberá justificar, conforme al Informe de Análisis de Impacto presentado por el solicitante, las actividades de evaluación que planea reutilizar y aquellas para las que considera necesario aplicar una regresión.

76. Teniendo en cuenta las justificaciones proporcionadas por el laboratorio, y atendiendo al Informe de Análisis de Impacto, el Organismo de Certificación podrá autorizar nuevas actividades de evaluación LINCE con una carga de esfuerzo menor o igual a las 25 jornadas/evaluador marcadas por la metodología LINCE, y por lo tanto autorizar la reutilización de las actividades previas. En todo caso, el esfuerzo máximo serán 25 jornadas/evaluador + 5 jornadas/evaluador por módulo opcional declarado en la ST, teniendo en cuenta las actividades re-utilizadas del expediente anterior y las nuevas actividades de evaluación planificadas.

77. Si tras el transcurso de la evaluación, el laboratorio verifica que las propiedades de seguridad establecidas en la declaración de seguridad se cumplen conforme a la metodología LINCE, el Organismo de Certificación podrá proponer una resolución estimatoria del expediente de certificación que culmine con la emisión del certificado LINCE para el TOE solicitado.

78. Los casos de renovación, re-certificación y mantenimiento serán realizados conforme a lo establecido en el [PO-005], la IT-002 y el documento de apoyo *Assurance Continuity: CCRA requirements [AC]*, que se consideran de aplicación a las evaluaciones LINCE.

4.9 VALIDEZ DEL CERTIFICADO

79. 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.

80. Se recomienda revisar la validez del certificado a los veinticuatro meses desde su emisión. El desarrollador podrá solicitar en cualquier momento la renovación del certificado o la re-certificación del producto, de acuerdo con lo establecido en el procedimiento [PO-005].

5. PUBLICIDAD

81. 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.

82. 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. GLOSARIO

83. **Declaración de seguridad (ST,** *Security Target***):** 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.
84. **Desarrollador:** persona o entidad que desarrolla, implementa o fabrica un objeto a evaluar. El término desarrollador indica la entidad que especifica, desarrolla, mantiene y/o fabrica el producto o alguno de sus componentes.
85. **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.
86. **Informe técnico de evaluación (ETR,** *Evaluation Technical Report***):** Informe emitido por el laboratorio de evaluación LINCE el cual resume los resultados de su evaluación.
87. **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.
88. **LINCE:** Certificación Nacional Esencial de Seguridad (LINCE).
89. **Objeto a evaluar (TOE,** *Target of Evaluation***):** 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.
90. **Organismo de Certificación: entidad acreditada por la Entidad Nacional de** Acreditación (ENAC) que expide certificaciones de seguridad TIC. En esta guía caso se refiere al organismo creado por el RD421/2004 y regulado por la Orden PRE/2740/2007.
91. **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.

7. REFERENCIAS

[AC]	Assurance Continuity: CCRA Requirements. Última versión aplicable publicada en: https://www.commoncriteriaportal.org
[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
[FOR-006]	Solicitud de cualificación de producto e inclusión en el catálogo de productos STIC (CPSTIC).
[PO-005]	PO-005 Certificación de productos.
[PO-006]	PO-006 Acreditación de laboratorios.
[PO-008]	PO-008 Certificación de productos en dominios técnicos

8. 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	Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, modificado por el Real Decreto 951/2015
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