GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN Centro Criptológico Nacional

Guía de Seguridad de las TIC
CCN-STIC 106

Procedimiento de inclusión de productos de seguridad TIC cualificados en el CPSTIC

Octubre 2017

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN Centro Criptológico Nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2017.10.05 15:42:16 +02'00'

NIPO: 785-17-038-8

Fecha de Edición: octubre de 2017.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

PRÓLOGO

El uso masivo de las tecnologías de la información y la comunicación (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, modificado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicación (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Octubre de 2017

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

ANEXOS

1. INTRODUCCIÓN

1. La adquisición de un producto de seguridad TIC que va a manejar información nacional clasificada o información sensible debe estar precedida de un proceso de comprobación de que los mecanismos de seguridad implementados en el producto son adecuados para proteger dicha información.
2. 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 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.
3. El Centro Criptológico Nacional (CCN) recibe múltiples consultas de los diferentes organismos de la Administración sobre qué productos deben emplear para proteger sus sistemas de las tecnologías de la información y la comunicación (TIC).
4. Para tratar de dar respuesta a estas consultas, el CCN publica la guía CCN-STIC 105 Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC) que ofrece un listado de productos STIC de referencia con el propósito de satisfacer las necesidades y demandas actuales de empleo de productos seguros en las redes de la Administración. El CPSTIC incluye los Productos Aprobados para manejar información nacional clasificada y los Productos Cualificados de Seguridad TIC.
5. La finalidad del CPSTIC es disponer de un listado de referencia de productos de seguridad TIC supervisado por el CCN que proporcione un nivel mínimo de confianza al usuario final en los productos adquiridos, con las mejoras de seguridad derivadas del proceso de evaluación y certificación, y en su empleo seguro en las redes de la Administración garantizado por un Procedimiento de Empleo.
6. Se recogerán en el apartado de Productos Aprobados de seguridad TIC en entornos clasificados aquellos que manejen información clasificada y en Productos Cualificados de Seguridad TIC para entornos sensibles o en aquellos sistemas de información de categoría alta en aplicación del ENS.
7. Para la inclusión de un producto en el catálogo, el CCN tendrá en cuenta una serie de criterios, como, la clasificación de la información que puede manejar (Difusión Limitada, Confidencial, Reservado, Secreto), las características de seguridad del producto, la categoría del sistema de información en el que puede emplearse (alta, media, básica[1]), las certificaciones aportadas, el entorno donde se vaya a emplear, etc. En función de esta información, se determinarán las

1 Clasificación por categorías definida en el ENS.

pruebas o evaluaciones que deberá superar el producto de seguridad TIC correspondiente.

8. El procedimiento para la inclusión de un producto STIC aprobado en el CPSTIC para manejar información nacional clasificada se describe en la guía CCN-STIC 102 Procedimiento para la Aprobación de Productos de seguridad TIC para manejar información Nacional clasificada [REF6]. La relación de la documentación y equipamiento a aportar para realizar la evaluación criptológica se describe en la CCN-STIC 130 Requisitos de Aprobación de Productos de Cifra para Manejar Información Nacional Clasificada [REF3] y para realizar la evaluación TEMPEST se describe en la guía CCN-STIC 151 Evaluación y Clasificación TEMPEST de equipos [REF5]. Ver Figura 1.

9. Así mismo, el procedimiento de inclusión de un producto de seguridad TIC cualificado en el CPSTIC se describe en la presente guía CCN-STIC 106, los requisitos fundamentales de seguridad o los perfiles de protección que deben cumplir los productos de seguridad TIC en función de su taxonomía se detallan en la guía CCN-STIC 140 Taxonomías de referencia para productos de seguridad TIC [REF8] y la descripción detallada del flujo, así como los tiempos máximos del proceso se describen en el Procedimiento de cualificación de productos STIC en el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI) PO-09 Procedimiento de cualificación de productos STIC en el ENECSTI [REF4]. Ver Figura 1.

10. El producto de seguridad TIC cualificado por el CCN hará referencia a una versión concreta y con una configuración determinada de acuerdo a unas normas de utilización que serán descritas en el procedimiento de empleo. Dicho procedimiento será distribuido por la empresa fabricante junto con el producto.

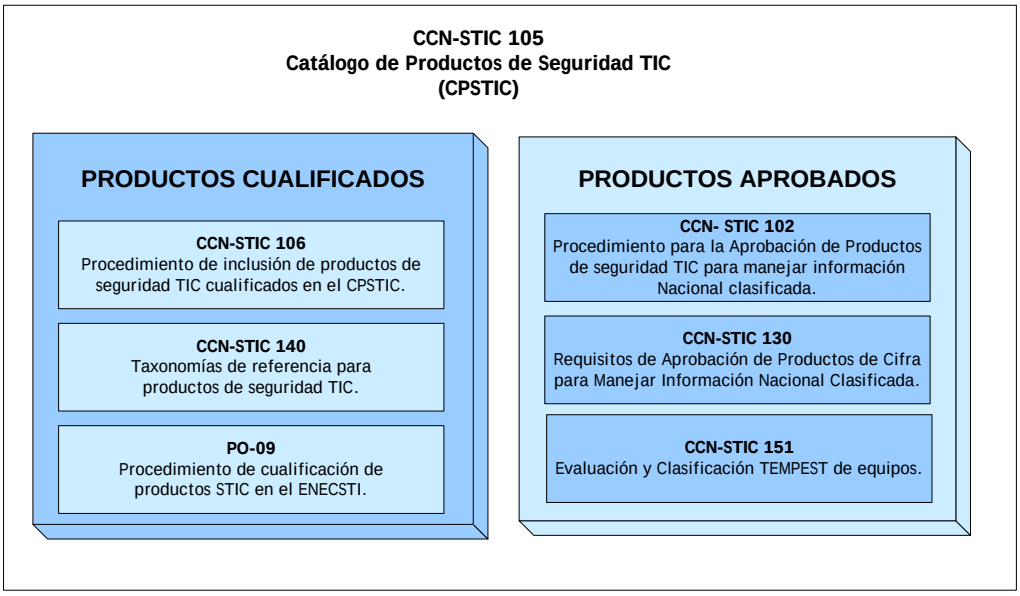

Figura 1. Inclusión de productos de seguridad en el CPSTIC.

2. OBJETIVO

11. El objeto del presente documento es definir el procedimiento y las evaluaciones requeridas a un producto de seguridad TIC[2] para ser incluido en el apartado de Productos Cualificados de Seguridad TIC, del Catálogo de Productos de Seguridad TIC (CPSTIC) [REF2].

12. Se entiende por producto de Seguridad TIC al conjunto de componentes software, firmware y/o hardware, que proporcionan funcionalidad de seguridad, diseñado para su uso o para su incorporación en un sistema o en un entorno operativo definido específicamente y con una utilidad particular.

3. ALCANCE

13. El Artículo 18 del RD 3/2010 de 8 de enero, modificado por el RD 951/2015, de 23 de octubre, por el que se regula el ENS en el ámbito de la administración electrónica dice:

    a) *"En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que vayan a ser empleados por las Administraciones públicas se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de Seguridad."*

    b) *"La certificación indicada en el apartado anterior deberá estar de acuerdo con las normas y estándares de mayor reconocimiento internacional, en el ámbito de la seguridad funcional."*

    c) *"El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información, constituido al amparo de lo dispuesto en el artículo 2.2.c) del Real Decreto 421/2004, de 12 de marzo, y regulado por la orden PRE/2740/2007, de 19 de septiembre, dentro de sus competencias, determinará el criterio a cumplir en función del uso previsto del producto a que se refiera, en relación con el nivel de evaluación, otras certificaciones de seguridad adicionales que se requieran normativamente, así como, excepcionalmente, en los casos en que no existan productos certificados. El proceso indicado, se efectuará teniendo en cuenta los criterios y metodologías de evaluación, determinados por las normas internacionales que recoge la orden ministerial citada."*

    d) *"Para la contratación de servicios de seguridad se estará a lo dispuesto en los apartados anteriores y en el artículo 15."*

[2] Según la definición del apartado **2.807 PRODUCTO DE SEGURIDAD TIC** de la REF1.

14. Para sistemas de información de categoría alta, el ENS establece la necesidad de utilizar componentes certificados:

    "*Componentes certificados [op.pl.5]*

dimensiones	todas		
categoría	básica	media	alta
	no aplica	no aplica	aplica

    Categoría ALTA
    Se utilizarán sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido evaluados conforme a normas europeas o internacionales y cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.
    Tendrán la consideración de normas europeas o internacionales, ISO/IEC 15408 u otras de naturaleza y calidad análogas.
    Una instrucción técnica de seguridad detallará los criterios exigibles."

15. Con el fin de facilitar a los organismos la labor de adquisición de productos STIC con la funcionalidad de seguridad certificada, los productos cualificados de seguridad TIC incluidos en el CPSTIC [REF2] podrán ser empleados como producto de seguridad en el Esquema Nacional de Seguridad.

16. El CCN se habrá encargado previamente de comprobar que el producto ha sido evaluado contra los Requisitos Fundamentales de Seguridad (RFS) de la taxonomía a la que pertenece el producto de seguridad (CCN-STIC 140 [REF8]) y que el certificado obtenido está reconocido por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información[3].

[3] Por ejemplo la norma Common Criteria, tiene consideración de norma internacional.

4. PROCEDIMIENTO DE INCLUSIÓN DE PRODUCTOS DE SEGURIDAD CUALIFICADOS EN EL CATÁLOGO DE PRODUCTOS (CPSTIC)

17. De una forma genérica, en la Figura 2, se puede ver el procedimiento de inclusión de productos cualificados en el Catálogo de Productos CPSTIC.

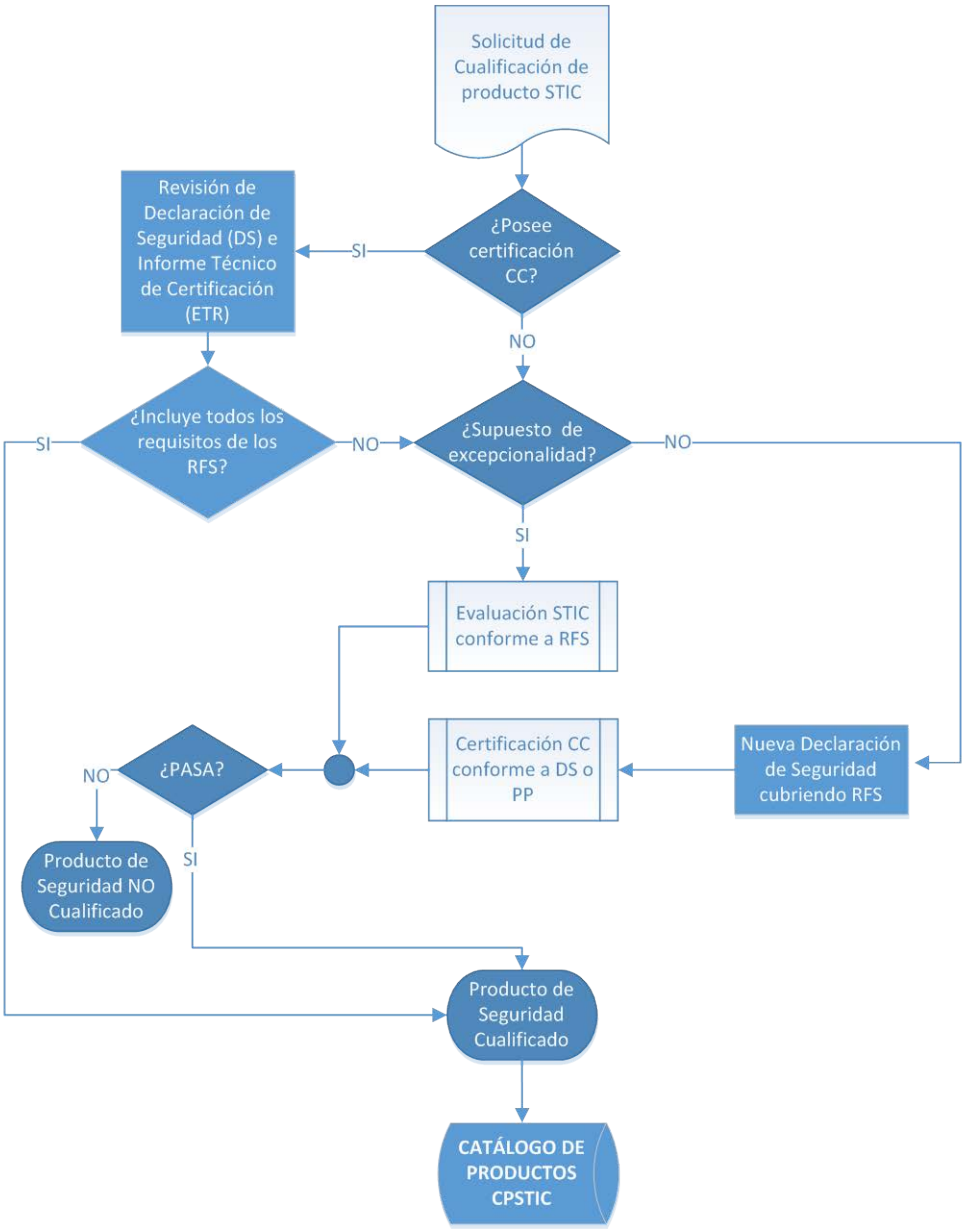

Figura 2. Procedimiento de inclusión de Productos de Seguridad Cualificados en el Catálogo de Productos (CPSTIC).

18. El proceso comienza con el envío al Organismo de Certificación (OC) del CCN de la solicitud de inclusión de un producto de seguridad como producto cualificado en el Catálogo de Productos CPSTIC (ver ANEXO A).

19. Esta solicitud la realizará preferiblemente el fabricante del producto STIC, también la podrá realizar un organismo de la Administración en el caso de que el producto cubra una necesidad operativa de dicho organismo y que no exista un producto equivalente en el Catálogo de Productos (CPSTIC).
20. Una solicitud realizada por un fabricante, podrá avalarse formalmente por un organismo de la Administración. Para ello, se rellenará el apartado Organismo Proponente del ANEXO A. Estas solicitudes con aval formal serán consideradas prioritarias por el CCN.
21. El producto de seguridad deberá ser catalogado dentro de una o varias familias de productos según la taxonomía definida por el Centro Criptológico Nacional en la CCN-STIC 140 [REF8]. Esta guía será publicada en la página web del Organismo de Certificación[4] y en el portal del CCN-CERT[5], y se actualizará periódicamente.
22. Dentro de esta taxonomía, se habrán especificado unos Requisitos Fundamentales de Seguridad (RFS), que serán una descripción detallada de las principales características de seguridad que deben tener todos los productos pertenecientes a dicha familia. Estos requisitos podrán haber sido definidos *ad-hoc* por el CCN para esa familia de productos o estar basados en un Perfil de Protección (PP) Common Criteria. Ver Anexos de la CCN-STIC 140 [REF8].
23. Junto a la solicitud de inclusión de un producto de seguridad TIC en el CPSTIC, se adjuntará:
    a) La Declaración de Seguridad (DS) o en su denominación inglesa *Security Target* (ST) de la certificación *Common Criteria*. La Declaración de Seguridad es un documento que refleja el análisis y propiedades de seguridad del objeto de evaluación y contiene los requisitos de seguridad y objetivos para un producto específico, así como las medidas funcionales y de garantía para cubrir los requisitos declarados.
    b) Una propuesta de procedimiento de empleo (PE) del producto.
    c) Un Informe Preliminar de Conformidad de los Requisitos Fundamentales de Seguridad (RFS). Este informe, realizado por el solicitante, consistirá en un análisis previo de las características de seguridad incluidas en la DS frente a las solicitadas en los RFS de la familia o familias de productos en los que se encuadra el producto candidato a entrar en el CPSTIC. En este informe de cumplimiento deberá indicarse claramente:
        i. Funcionalidades de seguridad de las requeridas en el documento de RFS incluidas en la DS.
        ii. Funcionalidades de seguridad requeridas en el documento de RFS no incluidas en la DS pero sí implementadas por el producto.

[4] https://oc.ccn.cni.es
[5] https://www.ccn-cert.cni.es

iii. Funcionalidades de seguridad requeridas en el documento de RFS no implementadas por el producto.

d) Listado de algoritmos criptológicos empleados en el producto.

24. En **casos excepcionales** (ver párrafo 28, caso 2), se podrá sustituir la DS por el Documento Detallado de Requisitos de Seguridad del producto (DDRS) (ver ANEXO B), que incluye la información que el Centro Criptológico Nacional necesita para poder determinar las pruebas o evaluaciones complementarias que se deberán realizar al producto.

25. Una vez revisada la solicitud por parte del Organismo de Certificación del CCN, y tras requerir la subsanación de cualquier defecto de forma que pueda presentar, se notificará al solicitante el inicio del proceso de inclusión de producto cualificado en el CPSTIC.

26. El personal asignado por el CCN al proceso de Cualificación revisará la documentación presentada por el solicitante y elaborará un "*Informe de Conformidad de Requisitos de Seguridad*".

27. En base a este informe, se determinará el grado de cumplimiento de los Requisitos Fundamentales de Seguridad exigibles al producto de seguridad con respecto a las evaluaciones/certificaciones de las que ya dispone el producto, y qué evaluaciones y pruebas complementarias se requerirán al producto para obtener la Cualificación de producto STIC.

28. En función de lo expuesto en el punto anterior, podrán darse los siguientes casos:

Caso 1: El producto de seguridad dispone de una certificación *Common Criteria* que cumple con TODOS los requisitos fundamentales de seguridad (RFS) mínimos exigidos.

En este caso se realizará una revisión básica del producto por parte del CCN, pero no se le exigirán evaluaciones adicionales (laboratorios externos). Tras finalizar satisfactoriamente la revisión del producto, el CCN realizará la propuesta formal de inclusión en el CPSTIC.

Caso 2: La Declaración de seguridad o DDRS del producto NO incluye todos los requisitos exigidos en los RFS y el producto cumple con los siguientes requisitos de excepcionalidad:

a) Que el producto no disponga de certificación CC o esta no incluya todos los requisitos de seguridad incluidos en los RFS y no exista la posibilidad de obtenerla al ser una solicitud promovida por un organismo de la Administración sin apoyo del fabricante.

b) Y que el producto sea considerado de interés estratégico para la Administración. Esta consideración será estudiada caso por caso por el Centro Criptológico Nacional e implica, entre otros factores, que no

exista otro producto disponible en el CPSTIC que cubra la misma necesidad operativa.

Se realizará una evaluación STIC (ver párrafo 45) por parte de un laboratorio acreditado en el ENECSTI, con el fin de verificar el cumplimiento de todos los requisitos RFS. El CCN realizará el seguimiento de la evaluación, y una vez finalizada satisfactoriamente, se realizará la propuesta formal de inclusión en el CPSTIC.

Caso 3: La Declaración de seguridad o DDRS del producto NO incluye todos los requisitos exigidos en los RFS y el producto no cumple con los requisitos de excepcionalidad.

En este caso se solicitará la recertificación CC basada en una nueva declaración de seguridad conforme a los RFS para la familia del producto o, si el CCN así lo considera, se podrá completar la certificación funcional que posee el producto con una evaluación STIC que realizará un laboratorio acreditado. El CCN realizará el seguimiento de la evaluación y una vez finalizada satisfactoriamente, se realizará la propuesta formal de inclusión en el CPSTIC.

29. En cualquier caso, si el producto de seguridad propuesto para su inclusión en el CPSTIC hiciera uso de algoritmos criptológicos, el CCN realizará la Validación de Algoritmos con la finalidad de valorar la seguridad criptológica de los algoritmos empleados, y su conformidad con los algoritmos de empleo en el ENS [REF7].
30. En el apartado 6 se pueden consultar las evaluaciones requeridas para la inclusión de un producto de seguridad en el Catálogo de Productos CPSTIC.
31. En el caso de productos que cuenten con una certificación previa, y que se encuentren en los casos 1 y 3 definidos anteriormente, el CCN se reserva del derecho de solicitar información adicional al solicitante para verificar si en el proceso de evaluación asociado a dicho certificado se han probado efectivamente todos los Requisitos Fundamentales de Seguridad definidos en la guía CCN-STIC 140 para la familia de productos para la que se solicita su inclusión.
32. Tras la superación satisfactoria de las evaluaciones requeridas, el CCN procederá a la inclusión del producto de seguridad, como Producto Cualificado, en el Catálogo de Productos de Seguridad de las TIC (CPSTIC) [REF2].
33. Además, se emitirá el certificado de **"Producto Cualificado de Seguridad TIC" que será firmada por el Secretario de Estado Director del Centro Nacional de Inteligencia**, que como Director del Centro Criptológico Nacional es la Autoridad de Certificación de la Seguridad de las Tecnologías de la Información (RD 421/2004 de 12 de Marzo, Art.1).
34. Se enviará una copia del certificado al fabricante junto con el Procedimiento de Empleo (PE) definitivo del producto de seguridad, tras haber sido revisado y

aprobado por el CCN. Dicho procedimiento de empleo deberá ser distribuido con el producto cada vez que sea adquirido.

35. El Catálogo de Productos de Seguridad de las TIC [REF2], que el CCN mantendrá actualizado, estará disponible en la página web del Organismo de Certificación del Centro Criptológico Nacional[6].

36. Cada nueva versión del producto cualificado requerirá de la validación de dicha versión por parte del CCN, para lo cual, el fabricante deberá entregar un informe de cambios y del impacto de dichos cambios en la seguridad del producto.

37. Una vez verificado que los cambios de la nueva versión garantizan las características de seguridad evaluadas del producto, se expedirá una adenda al certificado de Producto Cualificado de Seguridad TIC para dicha versión y se comunicará a través de los canales establecidos por el CCN. En caso contrario podría ser necesario volver a comenzar el proceso de cualificación para la nueva versión del producto.

38. Periódicamente el CCN realizará una revisión de las evaluaciones de los productos cualificados con el fin de garantizar la consistencia de sus características de seguridad en función de nuevas vulnerabilidades reportadas. Dicha revisión puede conllevar la revocación de la certificación de producto cualificado de seguridad si dejara de cumplir los mínimos requisitos exigidos.

5. EXCLUSIÓN DE UN PRODUCTO DEL CPSTIC

39. Un producto podrá ser excluido del CPSTIC por cualquiera de los siguientes motivos:

    a) Caducidad de su certificado de Producto Cualificado de Seguridad TIC. Todos los certificados de productos cualificados serán emitidos con una fecha de caducidad (que dependerá de la familia de productos considerada), a partir de la cual el solicitante deberá remitir una nueva solicitud de inclusión siguiendo el procedimiento descrito anteriormente. En el caso de que esta solicitud no se lleve a cabo, el CCN podrá excluir el producto del Catálogo de Productos CPSTIC.

    b) Revocación de la certificación Common Criteria (CC). En el caso de que fuese revocada la certificación CC de un determinado producto, éste podrá ser excluido del catálogo.

    c) Pérdida de las condiciones de excepcionalidad. En el caso de que el producto haya sido incluido en el catálogo por alguno de los supuestos de excepcionalidad, podrá ser excluido una vez deje de cumplirse alguno de ellos: aparición de productos sustitutivos con la certificación CC

[6] https://oc.ccn.cni.es

adecuada, pérdida de la consideración de producto estratégico para la administración, etc.

6. EVALUACIONES REQUERIDAS PARA LA INCLUSIÓN DE UN PRODUCTO DE SEGURIDAD CUALIFICADO EN EL CPSTIC

40. Las certificaciones y evaluaciones requeridas para que un producto de seguridad sea considerado Producto Cualificado dependerán de las certificaciones y evaluaciones previas que posea el producto y de la verificación de que éstas cubren los Requisitos Fundamentales de Seguridad (RFS).

41. Tras haber revisado los informes de las evaluaciones y certificaciones previas de las que disponga el producto de seguridad, el CCN elaborará un "Informe de Conformidad de Requisitos de Seguridad" en el que especificará las evaluaciones adicionales que se deberán realizar al producto para poder incluirlo en el CPSTIC como producto de seguridad cualificado.

42. A modo de resumen, en la Tabla 1 se pueden ver las evaluaciones requeridas para los productos de seguridad TIC cualificados.

CERTIFICACIONES PREVIAS	EVALUACIONES REQUERIDAS[7]	
	EVALUACIONES ADICIONALES	EVALUACIÓN CRIPTO
Certificación Common Criteria con TODOS RFS.	-	Validación algoritmos. Conformidad algoritmos de uso en el ENS.
Certificación Common Criteria no incluye TODOS RFS.	Recertificación Common Criteria o Evaluación STIC	
Sin Certificación Common Criteria	Certificación Common Criteria con todos RFS	

Tabla 1. Evaluaciones requeridas

43. En el caso de que el producto de seguridad se quiera emplear en sistemas de información de categoría alta según el ENS, será obligatorio dar cumplimiento a la medida de seguridad op.pl.5 Componentes Certificados (ver apartado 12)

44. La evaluación y certificación de un producto de seguridad TIC debe abarcar aspectos relativos a la implementación de los requisitos funcionales de

[7] Excepto casos de excepcionalidad.

seguridad en dicho producto, esto es, la evaluación *Common Criteria* y/o la evaluación STIC, o pruebas adicionales que permitan comprobar las funciones y mecanismos de seguridad del producto. Estas evaluaciones serán realizadas por **laboratorios acreditados en el ENECSTI**.

45. Una evaluación STIC es un conjunto de pruebas que deberá realizar un laboratorio con el fin de verificar el cumplimiento de todos los requisitos RFS. Estas pruebas consisten, entre otras, en un análisis vulnerabilidades, pruebas de caja negra y pruebas en entorno operacional.

46. En el caso de que el producto de seguridad TIC propuesto utilice algoritmos criptológicos, se deberán emplear aquellos que estén acreditados para su uso en el ENS, ver CCN-STIC 807 Criptología de Empleo en el ENS [REF7]. Además, el CCN realizará una validación de algoritmos con la finalidad de valorar la seguridad criptológica de los algoritmos empleados. Dicha validación se realizará una vez que el producto de seguridad haya finalizado satisfactoriamente la certificación funcional, en caso de que esta sea requerida.

7. REFERENCIAS

REF1	CCN-STIC 401 Glosarios y Abreviaturas.
REF2	CCN-STIC 105 Catálogo de Productos de Seguridad TIC (CPSTIC).
REF3	CCN-STIC 130 Requisitos de Aprobación de Productos de Cifra para Manejar Información Nacional Clasificada
REF4	PO-09 Procedimiento de cualificación de productos STIC el ENECSTI.
REF5	CCN-STIC 151 Evaluación y Clasificación TEMPEST de equipos.
REF6	CCN- STIC 102 Procedimiento para la Aprobación de Productos de seguridad TIC para manejar información Nacional clasificada.
REF7	CCN-STIC 807 Criptología de empleo en el ENS.
REF8	CCN-STIC 140 Taxonomías de referencia para productos de seguridad TIC.

8. ABREVIATURAS

CC	Criterios Comunes / *Common Criteria*
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación
DDRS	Documento Detallado de Requisitos de Seguridad
DS	Declaración de seguridad/Security Target
ENECSTI	Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.
ENS	Esquema Nacional de Seguridad
ETR	Evaluation Technical Report / Informe Técnico de Certificación
ITE	Informe Técnico de Evaluación
OC	Organismo de Certificación
PE	Procedimiento de Empleo
PP	Perfil de Protección
RD	Real Decreto
RFS	Requisitos Fundamentales de Seguridad
ST	Security Target / Declaración de Seguridad
STIC	Seguridad de las Tecnologías de la Información y la Comunicación
TIC	Tecnologías de la Información y la Comunicación

ANEXO A. FORMULARIO DE SOLICITUD DE INCLUSIÓN DE UN PRODUCTO DE SEGURIDAD COMO PRODUCTO CUALIFICADO EN EL CPSTIC

47. La última versión del formulario de solicitud de inclusión de un producto de seguridad como producto cualificado en el CPSTIC está disponible en la página web del Organismo de Certificación[8] para su descarga.

48. El formulario consta de los siguientes apartados:

    a) Datos del solicitante.

    b) Representante legal del solicitante.

    c) Persona de contacto.

    d) Organismo proponente (aval formal).

    e) Información del producto.

    f) Taxonomía del producto.

    g) Adjuntos (ficheros a adjuntar).

    h) Declaración de aceptar y conocer los requisitos de inclusión de productos de seguridad TIC cualificados.

49. Una vez cumplimentado, se deberá enviar al Organismo de Certificación en formato electrónico junto con los documentos anexos que procedan.

[8] https://oc.ccn.cni.es

ANEXO B. DOCUMENTO DETALLADO DE REQUISITOS DE SEGURIDAD (DDRS)

50. El DDRS especifica la información mínima de seguridad y funcionalidad del producto de seguridad TIC.

51. La información suministrada permitirá que el CCN tenga un conocimiento del producto y determine las pruebas o evaluaciones complementarias a las que deberá ser sometido para conseguir ser incluido en el CPSTIC.

52. Este documento sólo se aceptará si se cumplen las condiciones de Excepcionalidad definidas en el párrafo 28 caso 2 del presente documento.

53. El DDRS es una definición del problema de seguridad[9] en lenguaje natural que contendrá, al menos, los apartados incluidos en la primera parte de la Declaración de Seguridad (DS) en *Common Criteria*, es decir:

    a) Descripción de aquellas funcionalidades del producto que vayan a ser objeto de evaluación. Deberán incluir al menos los RFS definidos para la familia en la que se enmarca el producto.

    b) Descripción del problema de seguridad. Donde se incluirán:

        a. Descripción de los activos que se han de proteger.

        b. Descripción de las amenazas.

    c) Descripción del objetivo de seguridad.

[9] Declaración formal que define la naturaleza y el objetivo de seguridad que el producto intenta abordar, según definido en: www.commoncriteriaportal.org/cc Part1: Introduction and general model, Sección 4.