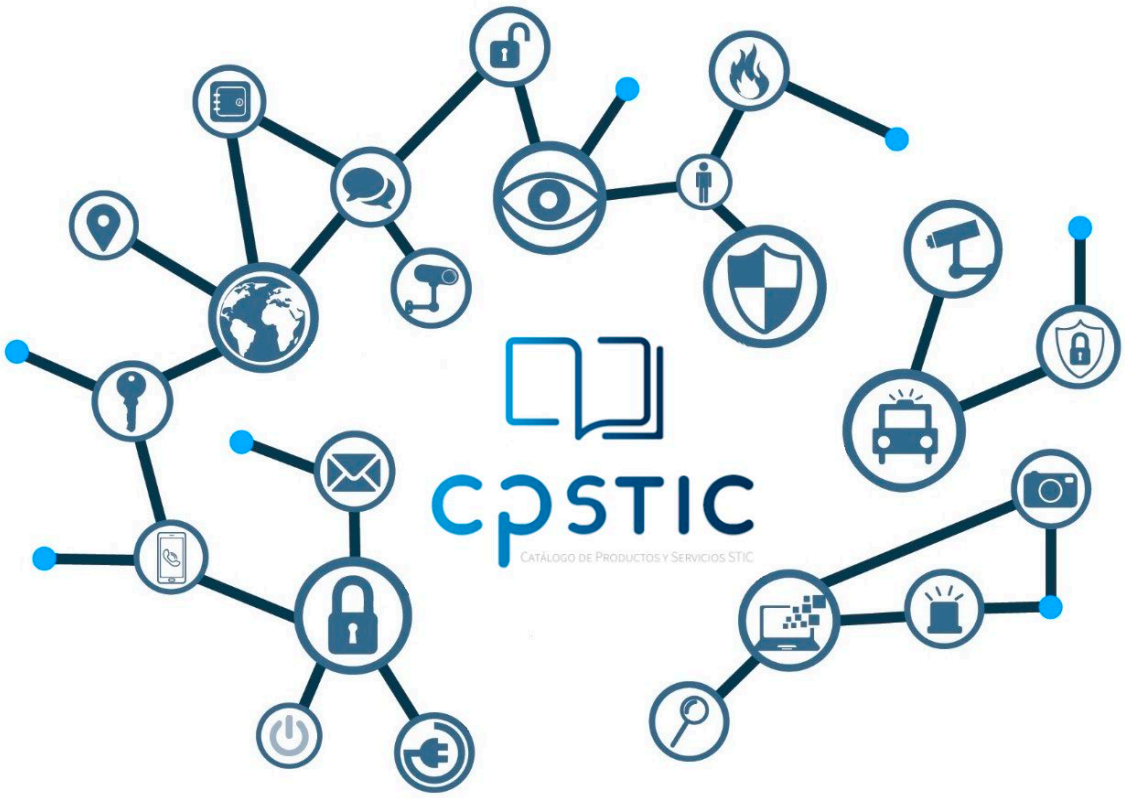
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 106

Procedimiento de inclusión de productos y servicios STIC cualificados en el CPSTIC



Abril 2024

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

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-143-3.
Fecha de Edición: abril de 2024

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
2024.04.11 18:09:34 +02'00'

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

ÍNDICE

ANEXOS

1. INTRODUCCIÓN

1. La adquisición de un producto o la contratación de un servicio 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 o servicio son adecuados para proteger dicha información.

2. La evaluación y certificación de un producto o servicio de seguridad TIC es el único medio objetivo que permite valorar y acreditar su capacidad 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. Así mismo, el Artículo 19, *Adquisición de productos de seguridad y contratación de servicios de seguridad*, del RD 311/2022 de 3 de mayo por el que se regula el ENS en el ámbito de la administración electrónica dice:

> *1. En la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en sistemas de información del ámbito de aplicación de este real decreto, se utilizarán, de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.*
>
> *2. El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información del Centro Criptológico Nacional, teniendo en cuenta los criterios y metodologías de evaluación nacionales e internacionales reconocidas por este organismo y en función del uso previsto del producto o servicio concreto dentro de sus competencias, determinará los siguientes aspectos:*
>
> *a) Los requisitos funcionales de seguridad y de aseguramiento de la certificación.*
>
> *b) Otras certificaciones de seguridad adicionales que se requieran normativamente.*
>
> *c) Excepcionalmente, el criterio a seguir en los casos en los que no existan productos o servicios certificados.*
>
> *3. Para la contratación de servicios de seguridad se estará a lo señalado en los apartados anteriores y a lo dispuesto en el artículo 16.*

4. Además, para sistemas de información de categoría **MEDIA y ALTA**, el ENS establece los siguientes requisitos:

– **[op.pl.5.1].** Se utilizará el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del CCN, para seleccionar los productos o servicios suministrados por un tercero que formen parte de la arquitectura de seguridad del sistema y aquellos que se referencien expresamente en las medidas de este real decreto.
En caso de que no existan productos o servicios en el CPSTIC que implementen las funcionalidades requeridas, se utilizarán productos certificados de acuerdo a lo descrito en el artículo 19.
Una Instrucción Técnica de Seguridad detallará los criterios relativos a la adquisición de productos de seguridad.

– **[op.pl.5.2]** Si el sistema suministra un servicio de seguridad a un tercero bajo el alcance del ENS, el producto o productos que en los que se sustente dicho servicio debe superar un proceso de cualificación y ser incluido en el CPSTIC, o aportar una certificación que cumpla con los requisitos funcionales de seguridad y de aseguramiento de acuerdo a lo establecido en el artículo 19.

5. Basándose en las competencias otorgadas por el RD 311/2022 de 3 de mayo y para dar respuesta a lo especificado en el artículo 19 y en su medida [op.pl.5], el CCN publica la guía **CCN-STIC 105 Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC)**.

6. Esta guía permite proporcionar un nivel mínimo de confianza al usuario final en los productos o servicios adquiridos, debido a las mejoras de seguridad derivadas del proceso de evaluación y certificación y a un procedimiento de empleo seguro.

7. El CPSTIC consta de tres (3) partes: **Productos Aprobados**, **Productos y Servicios Cualificados y Productos y Servicios de Conformidad y Gobernanza**. En el apartado de **Productos Aprobados** se recogen aquellos productos que se consideran adecuados para el manejo de información clasificada. En el apartado de **Productos y Servicios Cualificados** se incluyen aquellos que cumplen los requisitos de seguridad exigidos para el manejo de información sensible en el ENS, en cualquiera de sus categorías (ALTA, MEDIA y BÁSICA). Por último, en el apartado de Conformidad y Gobernanza se engloban soluciones que no pertenecen a la arquitectura de seguridad del sistema, pero implementan funcionalidades que facilitan el cumplimiento con la normativa de seguridad.

TIPO DE PRODUCTO O SERVICIO	INFORMACIÓN QUE MANEJA
APROBADO	CLASIFICADA
CUALIFICADO	SENSIBLE (ENS)
CONFORMIDAD Y GOBERNANZA DE LA SEGURIDAD	CUALQUIER TIPO

Tabla 1. Tipos de productos o servicios incluidos en el CPSTIC

8. Para la inclusión de un producto o servicio en el catálogo, el CCN tendrá en cuenta los siguientes criterios:

a) En el caso de **Productos Aprobados** para el manejo de información clasificada, el máximo nivel de clasificación de la información que puede manejar (DIFUSIÓN LIMITADA, CONFIDENCIAL, RESERVADO, SECRETO).

b) En el caso de **Productos y Servicios Cualificados**, la máxima categoría del sistema de información en el que puede emplearse (ALTA, MEDIA, BÁSICA[1]).

c) Las funcionalidades de seguridad que implementa el producto o servicio y las certificaciones aportadas.

d) Otros aspectos como el análisis de riesgos del producto o servicio, la necesidad operativa dentro de la Administración, la disponibilidad o no de otros productos o servicios certificados que satisfagan la misma funcionalidad, etc.

En función de esta información, se determinarán las pruebas o evaluaciones que deberá superar el producto o servicio de seguridad TIC correspondiente.

9. 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]. Los requisitos exigidos, la relación de la documentación y el 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].

10. Así mismo, el procedimiento de inclusión de un producto o servicio STIC cualificado en el CPSTIC se describe en la presente guía. Los requisitos fundamentales de seguridad que deben cumplir los productos o servicios de seguridad TIC en función de su taxonomía se detallan en los anexos de la guía **CCN-STIC 140 Taxonomías de referencia para productos y servicios de seguridad TIC** [REF8].

11. El producto o servicio STIC cualificado por el CCN hará referencia a una versión concreta, salvo en los casos especiales de servicios en la nube, y con una configuración determinada, de acuerdo a unas normas de utilización que serán descritas en un procedimiento de empleo seguro. Dicho procedimiento será distribuido por la empresa fabricante junto con el producto y además se publicará como una guía CCN-STIC de la serie 1000.

1 Clasificación por categorías definida en el ENS.

2. OBJETO Y ALCANCE

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

13. Se denomina **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.

14. Se denomina **servicio de Seguridad TIC** al servicio proporcionado por un determinado sistema TIC que aporta seguridad a la gestión y transferencia de información por parte de dicho sistema. Se materializa en la implementación de unos mecanismos de seguridad.

15. Con el fin de facilitar a los organismos la labor de adquisición de productos o contratación de servicios STIC con la funcionalidad de seguridad certificada, los productos y servicios cualificados STIC incluidos en el CPSTIC [REF2] podrán ser empleados como producto o servicio de seguridad en el ENS.

16. Para cada producto o servicio incluido en el CPSTIC, el CCN se habrá encargado previamente de comprobar que ha superado una evaluación que evidencia el cumplimiento de los Requisitos Fundamentales de Seguridad (RFS) de la taxonomía a la que pertenece el producto o servicio de seguridad (CCN-STIC 140 [REF8]) y que dispone de un procedimiento de empleo seguro.

[2] De acuerdo a la definición incluida en la guía CCN-STIC-401 [REF1].

3. PROCEDIMIENTO DE INCLUSIÓN DE PRODUCTOS DE SEGURIDAD CUALIFICADOS EN EL CPSTIC

17. De una forma genérica, en la Tabla 3, se puede ver el procedimiento de inclusión de productos cualificados en el CPSTIC.

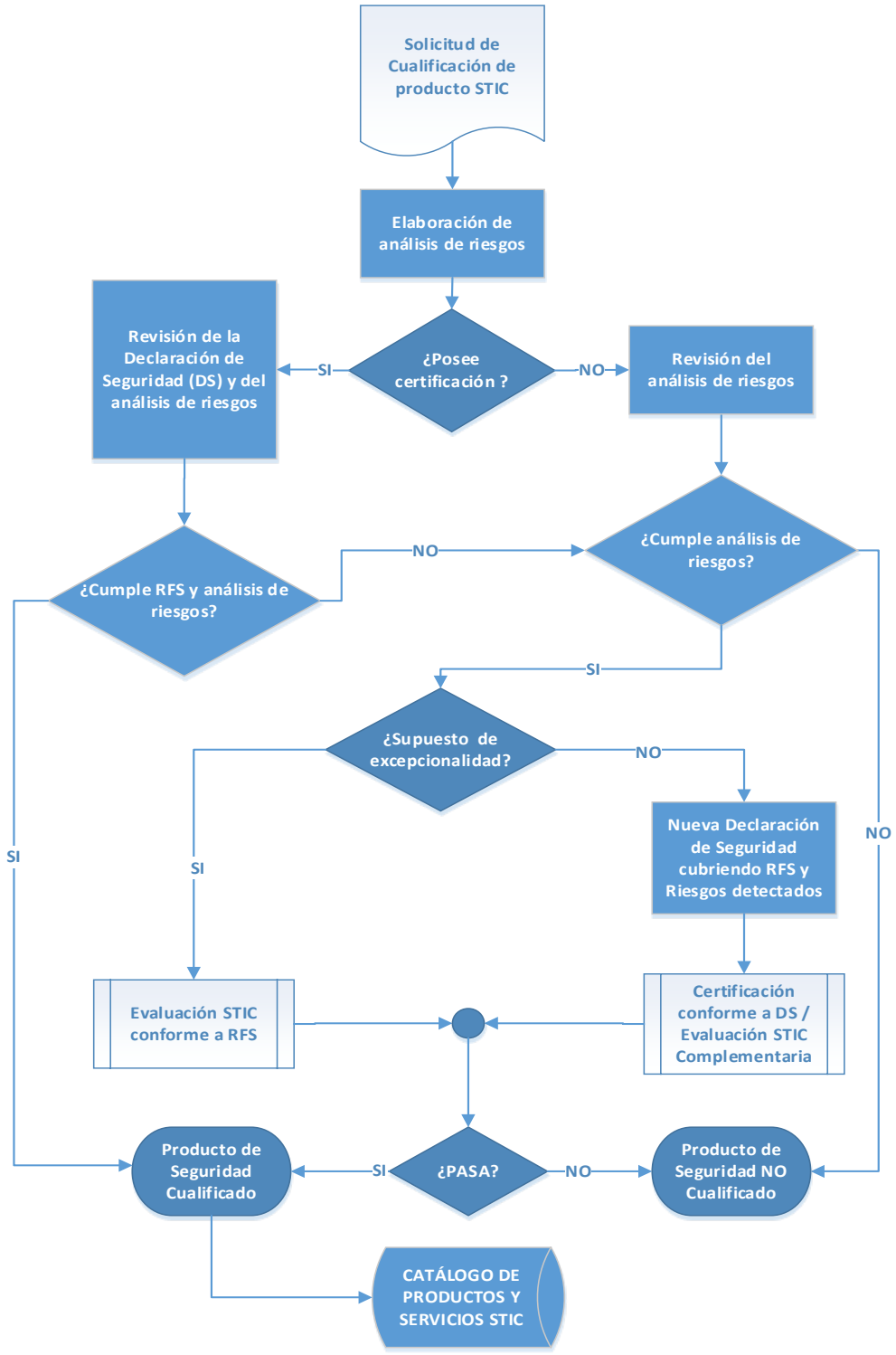


Figura 1. Procedimiento de inclusión de Productos de Seguridad Cualificados en el CPSTIC

18. Este procedimiento se aplicará a todos los productos candidatos a ser incluidos en el CPSTIC como producto Cualificado para cualquiera de las categorías del ENS (ALTA, MEDIA y BÁSICA). La diferencia fundamental es que para ENS Categoría ALTA se exigirá, de manera general, una certificación de acuerdo a la metodología *Common Criteria*, mientras que para los productos candidatos a entrar en las categorías de ENS MEDIA y BÁSICA, se exigirá, como mínimo, que dispongan de la Certificación Nacional Esencial de Seguridad (LINCE) [REF9].

19. El proceso comenzará con el envío al CCN[3] del formulario de solicitud de inclusión de un producto de seguridad como producto cualificado en el CPSTIC (ver ANEXO A). Existen dos (2) tipos de solicitud de inclusión: de nueva inclusión o de renovación. La primera está enfocada a la inclusión de un determinado producto y versión en el CPSTIC, mientras que solicitud de renovación se enviará cuando el producto ya se encuentre incluido, haya cumplido su fecha de renovación de cualificación y el fabricante desee mantener ese mismo producto y versión en el CPSTIC.

20. La solicitud de inclusión, sea del tipo que sea, la realizará el fabricante, un suministrador del producto STIC o un organismo de la Administración.

21. Una solicitud realizada por un fabricante o suministrador, podrá estar avalada formalmente por un organismo de la Administración. Para ello, se rellenará el apartado "Organismo Proponente" del formulario de solicitud. Estas solicitudes con aval formal serán consideradas prioritarias por el CCN.

22. Será obligatorio disponer de aval formal por parte de un organismo de la Administración en el caso de que el producto presentado cumpla con el caso 2 descrito en el párrafo 31 de esta guía (supuesto de excepcionalidad).

23. El producto de seguridad deberá ser catalogado dentro de una o varias familias de productos según la taxonomía definida por el CCN en la CCN-STIC 140 [REF8]. Esta guía será publicada en la página web del CPSTIC (https://cpstic.ccn.cni.es) y se actualizará periódicamente.

24. Dentro de esta taxonomía, se especifican unos Requisitos Fundamentales de Seguridad (RFS), que son una descripción detallada de las principales características de seguridad que deben tener todos los productos pertenecientes a dicha familia. Ver Anexos de la CCN-STIC 140 [REF8] (https://cpstic.ccn.cni.es/es/estructura).

25. **Cuando se trate de una nueva inclusión, junto a la solicitud de inclusión** de un producto de seguridad TIC en el CPSTIC, se adjuntará:

    a) La Declaración de Seguridad (DS)[4] de la certificación *Common Criteria* o LINCE, según el caso. 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.

[3] cpstic.ccn@cni.es

[4] En la metodología *Common Criteria* suele utilizarse su denominación inglesa: *Security Target (ST)*.

b) 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.

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

c) La política de versionado del producto, que describa el significado de cada uno de los caracteres que describen la versión, junto con la frecuencia y condiciones de actualización de cada uno de ellos.

d) Opcionalmente, el fabricante podrá adjuntar, con objeto de agilizar el análisis:

   i. Listado de algoritmos criptográficos empleados en el producto.

   ii. Una propuesta de procedimiento de empleo seguro (PES) del producto. La entrega de este documento será obligatoria una vez el producto sea incluido en el CPSTIC.

26. Una vez revisada la solicitud por parte 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 y se asignará un código de expediente de cualificación.

27. A continuación, el personal asignado por el CCN al proceso de Cualificación revisará la documentación presentada por el solicitante y realizará un análisis de riesgos complementario al planteado en los RFS de la familia correspondiente. En este análisis se determinarán, si los hubiera, aquellos riesgos no cubiertos por estos RFS.

28. Una vez finalizado el proceso de revisión y análisis de resultados, el CCN elaborará el "*Informe Técnico de Cualificación*" (ITC) y remitirá al fabricante las conclusiones del mismo en un documento denominado "Resultado del Informe Técnico de Cualificación" (RITC).

29. El RITC podrá ser FAVORABLE o DESFAVORABLE. En el caso de que el resultado sea DESFAVORABLE, en el RITC se describirá:

    a) el grado de cumplimiento de los RFS exigibles al producto con respecto a las evaluaciones/certificaciones de las que ya dispone.

    b) los riesgos derivados del análisis de riesgos complementario que no se encuentren cubiertos por la certificación.

c) las evaluaciones y pruebas complementarias (ver ANEXO E) que se requerirán al producto para obtener la cualificación de producto STIC.

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

Caso 1: El ITC determina que el producto cumple con TODOS los requisitos fundamentales de seguridad (RFS) mínimos exigidos y no existen riesgos derivados del análisis de riesgos complementario.

En este caso, el CCN realizará una revisión básica del producto, pero no se le exigirán evaluaciones adicionales (a través de laboratorios externos). Tras finalizar satisfactoriamente la revisión del producto, el CCN remitirá un RITC FAVORABLE al solicitante y realizará la propuesta de inclusión en el CPSTIC.

Caso 2: El ITC determina que el producto NO se encuentra dentro de los supuestos del Caso 1 y cumple con los siguientes requisitos de excepcionalidad:

a) No dispone de certificación CC o LINCE (según el caso).

b) No existen riesgos derivados del análisis de riesgos complementario realizado por el CCN.

c) Está considerado de interés estratégico para la Administración. Para ello, un organismo de la Administración deberá avalar y/o solicitar la cualificación, justificando dicha necesidad.

d) No existe en el CPSTIC otro producto con la misma funcionalidad que no se encuentre en el supuesto de excepcionalidad.

Esta consideración será estudiada caso por caso por el CCN. En caso de que el producto se encuentre dentro de este supuesto, un laboratorio acreditado en el ENECSTI realizará una evaluación STIC (ver párrafo 60), con el fin de verificar el cumplimiento de los RFS. El CCN realizará el seguimiento de la evaluación y remitirá el RITC al solicitante, cuyo resultado podrá ser FAVORABLE o DESFAVORABLE. En caso de que el resultado sea FAVORABLE, el CCN propondrá la inclusión del producto en el CPSTIC.

Caso 3: El producto no se encuentra dentro de los supuestos del Caso 1 ni del Caso 2 (no cumple con los requisitos de excepcionalidad).

En este caso, el CCN remitirá un RITC DESFAVORABLE, en el que se solicitará una nueva certificación CC o LINCE (según el caso) basada en una nueva declaración de seguridad conforme a los requisitos exigidos o se podrá completar la certificación funcional existente con una Evaluación STIC Complementaria en un laboratorio acreditado. El CCN realizará el seguimiento de la evaluación y remitirá el RITC al solicitante. En caso de que el resultado sea FAVORABLE, el CCN propondrá su inclusión en el CPSTIC.

31. En cualquier caso, si el producto de seguridad propuesto para ser incluido en el CPSTIC hiciera uso de algoritmos criptográficos, el CCN validará que dichos algoritmos presentan la seguridad criptológica requerida y se encuentran dentro de los algoritmos autorizados para el ENS [REF7].
32. En el apartado **6** de esta guía es posible consultar las evidencias requeridas para la inclusión de un producto de seguridad en el CPSTIC.
33. En el caso de las solicitudes en las que se aporten certificaciones, el CCN se reserva el derecho a solicitar información adicional para verificar si en el proceso de evaluación asociado a dicho certificado se han probado efectivamente todos los RFS definidos en la guía CCN-STIC 140 para la familia de productos para la que se solicita su inclusión.
34. Tras la superación satisfactoria de las evaluaciones requeridas, el CCN procederá a la inclusión del producto en el CPSTIC [REF2] como producto Cualificado. Esta inclusión se realizará de manera provisional hasta que el fabricante entregue, si no lo ha hecho previamente junto con la solicitud de inclusión, el Procedimiento de Empleo Seguro (PES) asociado al producto.
35. Además, se remitirá al solicitante una notificación de Resultado de Informe Técnico de Cualificación indicando el resultado del proceso. En caso de que el resultado sea favorable, el producto será incluido en el CPSTIC en la siguiente edición, no obstante, el producto se considerará cualificado desde el momento en que dicha notificación se remita al solicitante, aunque, por cuestiones editoriales, no aparezca todavía en el CPSTIC.
36. El CPSTIC, se publicará en formato:
    a) PDF en forma de guía CCN-STIC 105 [REF2]
    b) WEB en el sitio web https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic.
37. 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 Análisis de Diferencias (IAD), firmado por un responsable técnico, en el que se listen los cambios entre la versión que se pretende cualificar y la cualificada, así como una valoración de si impacta o no en alguno de los RFS evaluados.
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.

4. PROCEDIMIENTO DE INCLUSIÓN DE SERVICIOS DE SEGURIDAD CUALIFICADOS EN EL CPSTIC

39. De forma genérica, en la Figura 3 se puede ver el procedimiento de inclusión de servicios cualificados en el CPSTIC.

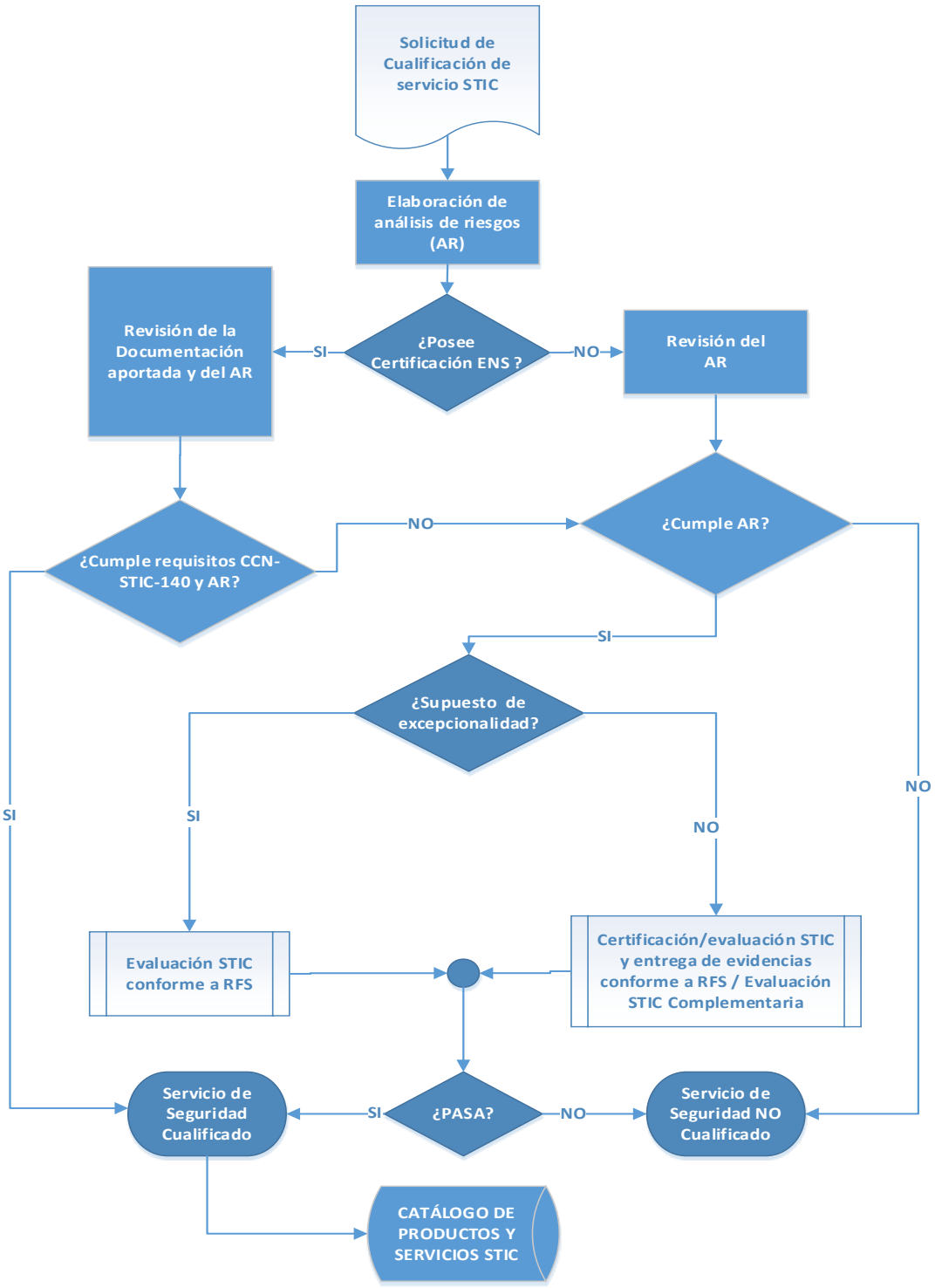


Figura 2. Procedimiento de inclusión de Servicios de Seguridad Cualificados en el CPSTIC

40. Este procedimiento se aplicará a todos los servicios en la nube candidatos a ser incluidos en el CPSTIC como servicio cualificado para las categorías del ENS (MEDIA y ALTA).

41. El proceso comenzará con el envío al CCN[5] de la solicitud de inclusión de un servicio de seguridad como servicio cualificado en el CPSTIC (ver ANEXO A). Esta solicitud la realizará el proveedor del servicio STIC o un organismo de la Administración.

42. Una solicitud realizada por un proveedor de servicio, podrá estar avalada formalmente por un organismo de la Administración. Para ello, se rellenará el apartado "Organismo Proponente" del formulario de solicitud. Estas solicitudes con aval formal serán consideradas prioritarias por el CCN.

43. El servicio de seguridad deberá ser catalogado dentro de una o varias familias según la taxonomía definida por el CCN en la CCN-STIC 140 [REF8]. Esta guía será publicada en la página web del CPSTIC (https://cpstic.ccn.cni.es).

44. 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 cumplir todos los servicios pertenecientes a dicha familia. Concretamente, cualquier servicio de seguridad en la nube deberá cumplir:

    a) Los requisitos RFS asociados a la funcionalidad principal del servicio, que serán los mismos que los asociados a un producto *on-premise* que desarrolle dicha funcionalidad (ver Anexos de la CCN-STIC 140 [REF8]). En este documento se establece, no solo una relación de los requisitos, sino los tipos de certificación y niveles exigidos, de acuerdo a lo indicado en el apartado **6**.

    Y

    b) Los requisitos adicionales aplicables a cualquier servicio genérico, incluidos en el Anexo G de la guía CCN-STIC-140 [REF8]. Estos requisitos aplican a servicios en la nube en cualquiera de sus tres modalidades (SaaS, PaaS e IaaS).

45. Junto a la solicitud de inclusión de un servicio de seguridad, se adjuntará:

    a) Referencia a la Certificación de Conformidad con el ENS e informe de auditoría elaborado por la entidad acreditada para ello.

    b) Documento de Arquitectura del Sistema (DAS) que ofrece el servicio en la nube que contenga:

        i. La estructura del TOE en términos de subsistemas, su comportamiento y los RFS que cada subsistema implementa. En el caso de que existan subsistemas del entorno operativo que implementen funcionalidades de seguridad requeridas en los RFS, también se incluirán y se identificará claramente que pertenecen al entorno, junto con los RFS que implementen.

        ii. Descripción de las interfaces de cada subsistema. Se identificarán claramente si son internas o externas.

[5] *cpstic.ccn@cni.es*

iii. Descripción de los flujos de aquella información que haya sido declarada entre los activos del sistema (por ejemplo: credenciales, claves, etc.). Concretamente, se definirá dónde se almacena y los canales por los que se transmite, indicando si es en claro o cifrado.

c) Declaración de Seguridad (DS) de la certificación asociada al producto que ofrece el servicio de seguridad en la nube o de la evaluación STIC a realizar, según proceda.

d) Declaración responsable de capacidad de suministro de logs (ver ANEXO B).

e) Informe de Transparencia con la información solicitada en el ANEXO G de la CCN-STIC-140 relativa a:

i. Herramientas de seguridad.

ii. Virtualización utilizada y mecanismos de segregación de datos.

iii. Mecanismos y procedimientos de borrado seguro de información.

iv. Ubicación geográfica de los datos.

f) Opcionalmente, con objeto de agilizar el análisis, el fabricante podrá adjuntar:

i. Listado de algoritmos criptográficos empleados en el suministro del servicio.

ii. Una propuesta de Procedimiento de Empleo Seguro (PES) del servicio. La entrega de este documento será obligatoria una vez el servicio sea incluido en el CPSTIC.

46. Una vez revisada la solicitud por parte 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 servicio cualificado en el CPSTIC.

47. El CCN revisará la documentación que acompañaba a la solicitud (la ST, el DAS, etc.) y, tras requerir la subsanación de cualquier defecto de forma que pueda presentar, se enviará al solicitante la notificación de validación de ST, que definirá el problema de seguridad y los requisitos que deben ser evaluados en laboratorio.

48. En la sección **6** de esta guía se puede consultar las evidencias requeridas para la inclusión de un servicio de seguridad en el CPSTIC.

49. Si el servicio de seguridad propuesto para ser incluido en el CPSTIC hiciera uso de algoritmos criptográficos, el CCN validará que dichos algoritmos presentan la seguridad criptológica requerida y se encuentran dentro de los algoritmos autorizados para el ENS [REF7].

50. En el caso de las solicitudes en las que se aporten certificaciones, el CCN se reserva el derecho a solicitar información adicional para verificar si en el proceso de evaluación/auditoría asociado a dicho certificado se han probado efectivamente los RFS definidos en la guía CCN-STIC 140 para la familia de servicios para la que se solicita su inclusión.

51. Tras la entrega y validación de las evidencias requeridas en lo que respecta al cumplimiento de los requisitos exigidos, el CCN remitirá al solicitante una notificación de Resultado de Informe Técnico de Cualificación (RITC) indicando el resultado del proceso y procederá a la inclusión del servicio en el CPSTIC [REF2] como servicio cualificado. Esta inclusión se realizará de manera provisional hasta que el fabricante entregue, si no lo ha hecho ya con la solicitud de inclusión, el PES asociado al servicio.

52. Se destaca que el servicio se considerará cualificado desde el momento en que la notificación RITC se remita al solicitante, independientemente de que, por cuestiones editoriales, no aparezca todavía en el CPSTIC.

53. Cada vez que el proveedor de servicio deba renovar la cualificación el proveedor de servicio deberá remitir al CCN una nueva solicitud, y se reiniciará el proceso de cualificación del servicio como si se tratase de una nueva inclusión.

54. Periódicamente, el CCN realizará una revisión de las evaluaciones de los servicios 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 del servicio cualificado de seguridad si dejara de cumplir los mínimos requisitos exigidos.

5. EXCLUSIÓN DE UN PRODUCTO O SERVICIO DEL CPSTIC

55. Un producto o servicio podrá ser excluido del CPSTIC por cualquiera de los siguientes motivos:

    a) Alcance de la fecha de revisión de validez para el Producto o Servicio Cualificado STIC. Una vez que un producto o servicio alcance su fecha de revisión de validez, el solicitante deberá remitir una nueva solicitud de inclusión siguiendo el procedimiento descrito anteriormente para cada caso. En el caso de que esta solicitud no se lleve a cabo, el CCN podrá excluir el producto o servicio del CPSTIC.

    b) Revocación o caducidad de alguna de las certificaciones requeridas al producto o servicio para acceder al catálogo: *Common Criteria*, LINCE, conformidad con el ENS, según el caso. Para las certificaciones *Common Criteria* o LINCE se considerará, como máximo, una validez de 5 años.

    c) Pérdida de las condiciones de excepcionalidad. En el caso de que el producto o servicio 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 o servicios sustitutivos con la certificación adecuada, pérdida de la consideración de producto o servicio estratégico para la Administración, etc.

    d) Que no cumpla con los RFS vigentes en el momento de la revisión de validez. Los avances tecnológicos pueden dejar obsoleta la tecnología empleada en unos casos y en otros hacer que se reduzca de forma considerable la seguridad del mismo, lo que implicará una evolución de los RFS.

    e) Que presente vulnerabilidades críticas no corregidas. En este caso, podrá solicitarse al fabricante un informe de impacto de dichas vulnerabilidades. Si este informe determinase que la vulnerabilidad es explotable siguiendo el PES, este será excluido del catálogo.

    f) Que el fabricante no haya entregado la propuesta de Procedimiento de Empleo Seguro en el periodo de inclusión provisional.

    g) Que haya finalizado el soporte de seguridad por parte del fabricante. En este caso, el fabricante estará obligado a notificar al CPSTIC que los productos que se encuentran cualificados han perdido dicho soporte.

6. EVIDENCIAS REQUERIDAS PARA LA CUALIFICACIÓN DE UN PRODUCTO O SERVICIO STIC

56. Las certificaciones y evaluaciones requeridas para que un producto o servicio de seguridad sea considerado Cualificado dependerán de:

    a) Las certificaciones y evaluaciones previas que posea el producto o servicio.

    b) La verificación de que estas cubren los Requisitos Fundamentales de Seguridad (RFS).

    c) El resultado del análisis de riesgos complementario realizado por el CCN.

57. Tras haber revisado los informes de las evaluaciones y certificaciones previas de las que disponga el producto o servicio de seguridad, el CCN elaborará el "Informe Técnico de Cualificación" (ITC) en el que especificará las evidencias adicionales que el fabricante o proveedor de servicio deberá entregar para que pueda ser incluido en el CPSTIC como producto o servicio de seguridad cualificado. El resultado de este ITC se le comunicará al fabricante mediante el RITC.

58. A modo de resumen, en la Tabla 2 y la Tabla 3 se pueden ver las evidencias requeridas a los **productos STIC cualificados**.

EVIDENCIAS REQUERIDAS PARA CUALIFICACIÓN DE PRODUCTOS ENS ALTA		
CERTIFICACIONES PREVIAS	**EVALUACIONES**[6]	
	EVALUACIONES ADICIONALES	**EVALUACIÓN CRIPTO**
Certificación *Common Criteria* incluye TODOS RFS.	Dependerá del análisis de Riesgos	Validación algoritmos. Conformidad algoritmos de uso en el ENS Categoría ALTA.
Certificación *Common Criteria* no incluye TODOS RFS.	Recertificación *Common Criteria* o Evaluación STIC Complementaria	
Sin Certificación *Common Criteria*	Certificación *Common Criteria* con todos RFS	

Tabla 2. Evidencias requeridas para cualificación ENS categoría ALTA

[6] Excepto casos de excepcionalidad.

EVIDENCIAS REQUERIDAS PARA PRODUCTOS ENS MEDIA Y BÁSICA		
CERTIFICACIONES PREVIAS	**EVALUACIONES REQUERIDAS**[7]	
	EVALUACIONES ADICIONALES	**EVALUACIÓN CRIPTO**
Certificación *Common Criteria* o LINCE incluye TODOS RFS.	Dependerá del análisis de Riesgos	Validación algoritmos. Conformidad algoritmos de uso en el ENS Categoría MEDIA y BÁSICA
Certificación *Common Criteria* no incluye TODOS RFS.	Evaluación STIC Complementaria	
Sin Certificación	Certificación LINCE con todos RFS	

Tabla 3. Evidencias requeridas para ENS categoría MEDIA y BÁSICA

59. En la Tabla 4 se pueden ver las evidencias requeridas a los **servicios STIC cualificados**.

EVIDENCIAS REQUERIDAS PARA CUALIFICACIÓN DE SERVICIOS		
CERTIFICACIONES	**EVALUACIONES**[8]	
	EVALUACIONES ADICIONALES	**EVALUACIÓN CRIPTO**
Caso 1: 1) Certificación de Conformidad con el ENS 2) Certificación de producto	Cumplimiento con RFS del Anexo G de la CCN-STIC-140, incluyendo Auditoría de *Pentesting*	Validación algoritmos. Conformidad algoritmos de uso en el ENS de acuerdo a la categoría solicitada
Caso 2: 3) Certificación de Conformidad con el ENS 4) Evaluación STIC (ver ANEXO H)	Cumplimiento con RFS del Anexo G de la CCN-STIC-140, sin incluir auditoría de *Pentesting*	

Tabla 4. Evidencias requeridas para cualificación de servicios

[7] Excepto casos de excepcionalidad.
[8] Excepto casos de excepcionalidad.

60. Las evaluaciones STIC complementarias (ver ANEXO E), las evaluaciones STIC (ANEXO H), las certificaciones LINCE y las auditorías de *pentesting* serán realizadas por **laboratorios acreditados en el ENECSTI**.

61. En el caso de que el producto o servicio de seguridad TIC propuesto utilice algoritmos criptológicos, se deberán emplear aquellos que estén autorizados para su uso en el ENS (ver CCN-STIC 807 Criptología de Empleo en el ENS [REF7]). Además, el CCN validará que dichos algoritmos presentan la seguridad criptológica requerida y se encuentran dentro de los algoritmos autorizados para el ENS [REF7].

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

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.

REF9 CCN-STIC 2001 Definición de la Certificación Nacional Esencial de Seguridad (LINCE)

8. ABREVIATURAS

CC	Criterios Comunes / Common Criteria
CCN	Centro Criptológico Nacional
CETR	*Complementary Evaluation Technical Report* / Informe Técnico de Evaluación Complementaria
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación
CSP	Cloud Service Provider / Proveedor del servicio *cloud*
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
IAD	Informe de Análisis Diferencial
ITC	Informe Técnico de Cualificación
ITE	Informe Técnico de Evaluación
OC	Organismo de Certificación
PES	Procedimiento de Empleo Seguro
PP	Perfil de Protección
RD	Real Decreto
RFS	Requisitos Fundamentales de Seguridad
RITC	Resultado del Informe Técnico de Cualificación
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

TOE *Target of evaluation*

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

62. Para iniciar el proceso de cualificación, el solicitante deberá rellenar el formulario de "Solicitud de cualificación de producto e inclusión Catálogo de Productos y Servicios STIC (CPSTIC)" (FOR-CPSTIC-003), o bien el formulario de "Solicitud de cualificación de servicio e inclusión Catálogo de Productos y Servicios STIC (CPSTIC)" (FOR-CPSTIC-005), según se trate de un producto o servicio, ambos disponibles en el apartado "Inclusión" de la página web del CPSTIC[9].

63. El formulario consta de los siguientes apartados:

    a) Tipo de solicitud: nueva solicitud / renovación.

    b) Datos del solicitante.

    c) Persona de contacto.

    d) Organismo proponente (aval formal).

    e) Información del producto o servicio.

    f) Certificación *Common Criteria*, LINCE o Certificación de Conformidad con el ENS, según se trate de un producto o un servicio.

    g) Laboratorio con el que se haya contratado la evaluación, si aplica.

    h) Taxonomía del producto o servicio.

    i) Categoría del ENS para la que se solicita la cualificación (ALTA o MEDIA).

    j) Adjuntos (ficheros a adjuntar).

    k) Declaración de que toda la información contenida en el formulario es veraz y completa.

64. Una vez cumplimentado el formulario, se deberá enviar al CCN (cpstic.ccn@cni.es) junto con los anexos que procedan y la "*Declaración responsable para la cualificación de productos/servicios STIC*" (FOR-CPSTIC-001) disponible en el mismo apartado de la web del CPSTIC. El documento de solicitud deberá mantener los campos de formulario que originariamente tenía para que la solicitud se considere válida.

[9] https://cpstic.ccn.cni.es/es/inclusion

ANEXO B. DECLARACIÓN RESPONSABLE DE CAPACIDAD DE SUMINISTRO DE LOGS

65. A continuación, se describe el contenido de la declaración de estar en disposición de ofrecer al cliente la información requerida relativa a los *logs* generados por su uso del servicio.

66. La declaración debe constar de los siguientes apartados:

    a) Razón social del proveedor del servicio *cloud* (CSP) y su número de identificación fiscal.

    b) Identificación unívoca del servicio.

    c) Declaración de estar en disposición de ofrecer al cliente:

        - la información requerida relativa a los *logs* generados por su uso del servicio.

        - únicamente la información de sus *logs*, sin revelar información adicional o de otros clientes.

    d) Firma del representante del CSP.

ANEXO C. DISTINTIVO DE PRODUCTO O SERVICIO CUALIFICADO

67. La cualificación de un producto/servicio para el ENS podrá representarse mediante el **Distintivo de Producto Cualificado** o el **Distintivo de Servicio Cualificado**, que serán expedidos por el CCN, y cuyo uso por parte del solicitante del proceso de cualificación (que, salvo excepciones, será el fabricante) estará condicionado a la inclusión del producto/servicio en el CPSTIC.

68. En adelante, denominaremos **distintivos de cualificación**, de manera genérica, al **Distintivo de Producto Cualificado** y al **Distintivo de Servicio Cualificado**.

69. El solicitante del proceso de cualificación podrá, de forma voluntaria, dar publicidad a los productos/servicios cualificados mediante la exhibición de cualquiera de los distintivos de cualificación en su documentación técnica o comercial, en cualquiera de sus formatos (web, papel, etc…).

70. Los distintivos de Producto y Servicio Cualificado se encuentran en la sección "MEDIA" de la página web del CPSTIC.

71. Queda expresamente prohibida la manipulación o reproducción parcial de los distintivos de cualificación, así como la utilización de este último sin que quede expresamente indicado a qué producto/servicio está asociado.

72. En los casos en los que se incumpla el apartado anterior, el CCN requerirá la rectificación inmediata del error y/o la retirada de los distintivos de cualificación. Además, el CCN podrá decidir retirar el producto/servicio o conjunto de productos/servicios de dicho solicitante del CPSTIC cuando detecte que este ha hecho un uso fraudulento de los distintivos de cualificación.

73. Una vez se haya procedido a la exclusión de un producto/servicio del CPSTIC, debido a cualquiera de los motivos expresados en el apartado **5** de la presente guía, el solicitante del proceso de cualificación deberá retirar cualquier distintivo de cualificación utilizado dentro de la documentación de dicho producto/servicio.

C.1. DISTINTIVO DE PRODUCTO CUALIFICADO

74. El **Distintivo de Producto Cualificado** tendrá el aspecto y contenido que se muestra en las figuras siguientes, incluyendo la categoría máxima para la que el producto está cualificado. (MEDIA o ALTA)[10].

Figura 3. Distintivo de Producto Cualificado Categoría ALTA

Figura 4. Distintivo de Producto Cualificado Categoría MEDIA

UTILIZACIÓN DE PRODUCTOS EN EL ENS DE ACUERDO AL DISTINTIVO	
CUALIFICACIÓN OBTENIDA	**ADECUADO PARA SISTEMAS**
ALTA	ENS Cat. ALTA ENS Cat. MEDIA ENS Cat. BÁSICA
MEDIA	ENS Cat. MEDIA ENS Cat. BÁSICA

Tabla 5. Utilización de productos en el ENS de acuerdo al distintivo

[10] De momento, no está prevista la cualificación de productos únicamente para categoría BÁSICA.

C.2. DISTINTIVO DE SERVICIO CUALIFICADO

75. El **Distintivo de Servicio Cualificado** tendrá el aspecto y contenido que se muestra en las figuras siguientes, incluyendo la categoría máxima para la que el servicio está cualificado. (MEDIA o ALTA)[11].

Figura 5. Distintivo de Servicio Cualificado Categoría ALTA

Figura 6. Distintivo de Servicio Cualificado Categoría MEDIA

UTILIZACIÓN DE SERVICIOS EN EL ENS DE ACUERDO AL DISTINTIVO	
CUALIFICACIÓN OBTENIDA	**ADECUADO PARA SISTEMAS**
ALTA	ENS Cat. ALTA ENS Cat. MEDIA ENS Cat. BÁSICA
MEDIA	ENS Cat. MEDIA ENS Cat. BÁSICA

Tabla 6. Utilización de servicios en el ENS de acuerdo al distintivo

[11] De momento, no está prevista la cualificación de servicios únicamente para categoría BÁSICA.

ANEXO D. ESTRATEGIA DE CUALIFICACIÓN CONTINUA

76. El proceso de cualificación descrito hasta el momento en el presente documento consiste en la validación, por parte del CCN, de que un determinada versión de un producto[12] cumple con los Requisitos Fundamentales de Seguridad descritos en el anexo correspondiente a la familia o familias de la CCN-STIC-140 en las que se enmarca.

77. Esta validación está basada en la certificación aportada por el producto, que se completará con la validación de que los algoritmos criptológicos utilizados se encuentran dentro de los autorizados por el CCN en la guía CCN-STIC-807 y, en caso necesario, en una Evaluación STIC Complementaria.

78. No obstante, los procesos de evaluación asociados a dichas certificaciones suelen ser largos y, en ocasiones, incompatibles con el ciclo de vida de la versión certificada del producto. Un caso extremo sería, por ejemplo, la dificultad de certificar bajo la metodología *Common Criteria* un producto desarrollado utilizando el modelo DevOps, ampliamente utilizado hoy en día para entornos del *cloud*, ya que posiblemente el producto habría finalizado su ciclo de vida al término de la certificación.

79. Para solventar esta situación, partiendo de la base de que un objetivo primordial del CPSTIC es ofrecer un **listado actualizado** de productos, se plantea la **Estrategia de Cualificación Continua**, que pretende agilizar la cualificación e inclusión en el Catálogo de productos que no se corresponden con los certificados pero que presentan **diferencias menores** con respecto a estos (nuevas versiones *firmware*, nuevos modelos *hardware*, etc.).

80. La Figura 8 representa como sería el proceso de cualificación de un producto que presente diferencias menores con respecto a uno certificado. En este caso, se evaluarían las diferencias desde distintos puntos de vista o dimensiones:

    a. Evaluación de nuevas funcionalidades de seguridad implementadas por el producto que afecten a los RFS definidos para la familia a la que pertenece. Este sería el caso de un producto que, por ejemplo, incluya en los RFS la funcionalidad de Identificación y Autenticación y haya añadido un nuevo método de Identificación y Autenticación con respecto a los utilizados por el producto certificado. Las actividades de evaluación asociadas a este caso se describen en el ANEXO E.

    b. Evaluación de nuevos modelos *hardware*. Este sería el caso en el que en la certificación original se hayan incluido una serie de modelos *hardware* sobre los que corre un *software/firmware* determinado y se desee ampliar este conjunto de modelos. Las actividades de evaluación se corresponderían a las de evaluación de series de productos descritas en el ANEXO F.

[12] Aunque todo lo descrito en el presente anexo es aplicable tanto a productos como a servicios, por economía del lenguaje nos referiremos en adelante de manera genérica a “productos”.

c. Reevaluación de funcionalidades incluidas en los RFS definidos para la familia a la que pertenece el producto que hayan sufrido modificaciones. Las actividades de evaluación asociadas a este caso se describen el en ANEXO G.

81. La evaluación final podría contener las tres (3) dimensiones o una combinación de ellas, según corresponda.

Figura 7. Evaluaciones asociadas al proceso de cualificación de un producto que presente diferencias menores con respecto a uno certificado

82. El Proceso Cualificación Continua, enmarcado en la Estrategia de Cualificación Continua, consiste en un proceso de duración indefinida en el tiempo en el cual se cualifican todas aquellas versiones menores o modelos *hardware* no incluidos en la certificación de partida.

83. Se denomina iteración a cada una de las evaluaciones asociadas a dicho proceso. Para que la cualificación continua sea posible, será necesario que los distintos modelos y/o versiones menores del producto asociados a cada iteración hayan superado con éxito las evaluaciones descritas en el párrafo anterior.

84. La Figura 9 muestra un esquema del proceso de evaluación continua de N iteraciones.

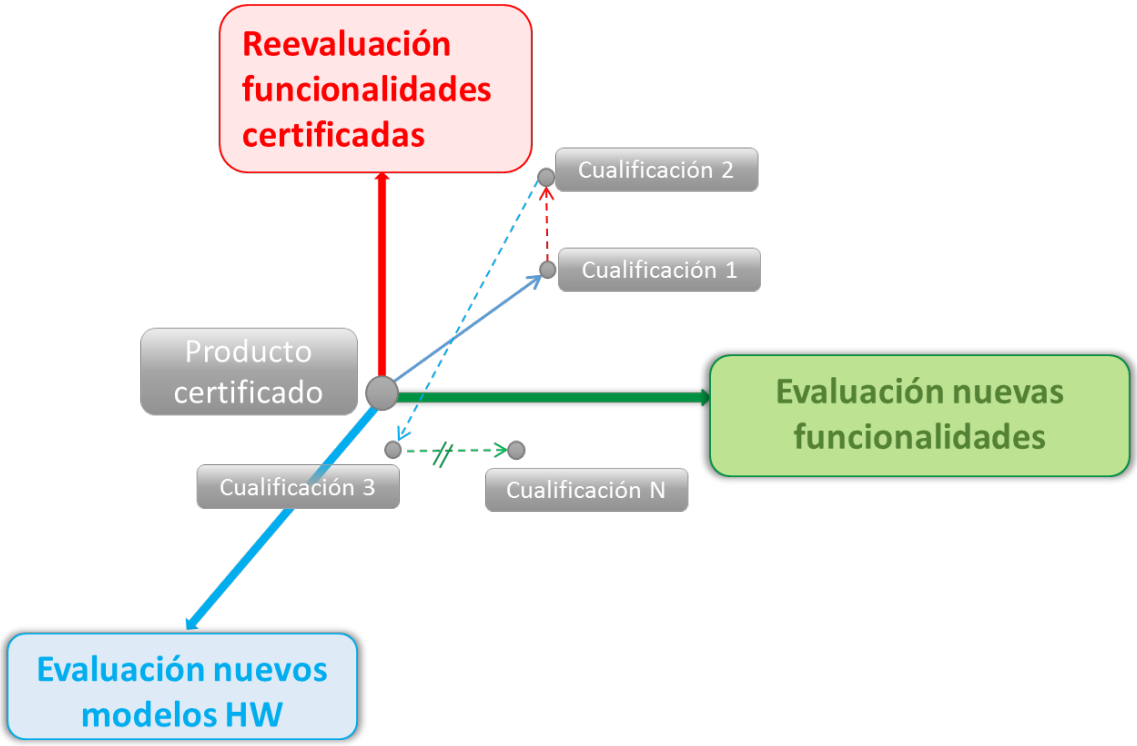


Figura 8. Evaluaciones asociadas al proceso de cualificación continua de un producto

ANEXO E. EVALUACIONES STIC COMPLEMENTARIAS

85. Este Anexo establece los pasos necesarios para la realización de Evaluaciones STIC Complementarias basadas en la metodología LINCE.

86. Este tipo de evaluaciones se denominan Complementarias porque son exigidas cuando un producto candidato a ser incluido en el CPSTIC presenta una certificación que no cubre todos los requisitos exigidos en el anexo de la CCN-STIC-140 correspondiente a la familia a la que pertenece.

87. El objetivo de este proceso de evaluación es permitir a un laboratorio verificar si el producto cumple los requisitos de seguridad exigidos que no hayan sido incluidos en la certificación inicial y que, por tanto, deben ser específicamente evaluados para determinar la efectividad de las funciones de seguridad implementadas.

88. El resultado de la Evaluación STIC Complementaria se incluirá en el Informe Técnico de Evaluación Complementaria (CETR, *Complementary Evaluation Technical Report).*

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

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

E.1. EVIDENCIAS MÍNIMAS NECESARIAS

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

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

    a) Declaración de Seguridad (ST).

    b) Guías de operación e instalación del TOE (*Common Criteria*).

    c) Entorno de ejecución del TOE.

E.2. DECLARACIÓN DE SEGURIDAD

93. La Declaración de Seguridad (ST) se utiliza para especificar la funcionalidad de seguridad del producto/servicio que será evaluado y para describir las distintas relaciones entre el producto/servicio y el entorno en el cual será utilizado.

94. La ST deberá contener:

a) Información del patrocinador, TOE y evaluación. Tal como se describe en el apartado correspondiente de la guía CCN-STIC-2003.

b) Descripción funcional del TOE y su entorno de ejecución. Cuando el entorno se describe de forma general y el producto se ejecuta sobre una plataforma, el evaluador no tiene la obligación de probarlo en todas las plataformas posibles. Se detallará en qué plataforma específica se realiza la evaluación.

c) Hipótesis sobre el entorno de ejecución. Esto determinará el alcance de la evaluación, puesto que, dependiendo de las hipótesis que se realicen, algunos posibles ataques pueden quedar fuera del alcance de la evaluación. Dado que el objeto de este tipo de evaluaciones es completar las realizadas dentro del alcance de una certificación, las hipótesis sobre el entorno deberán ser, por defecto, las mismas que las consideradas en la certificación. Cualquier modificación deberá ser debidamente justificada y autorizada por el CCN.

d) Especificación de las funcionalidades de seguridad del producto objeto de evaluación. Los requisitos de seguridad que serán incluidos en la ST son aquellos que el CCN determine que no han sido cubiertos por la certificación de seguridad ya obtenida por el producto/servicio. Por ello, esta ST deberá ser validada por el CCN, con anterioridad al inicio de la evaluación asociada.

E.3. PROCEDIMIENTO DE EVALUACIÓN

95. El este punto se establece el criterio de evaluación con el cual se pretende verificar la conformidad y la resistencia de las funcionalidades de seguridad incluidas en la ST de la Evaluación STIC Complementaria.

96. A continuación, se describen las distintas etapas a realizar:

a) Etapa 1 – Análisis de la Declaración de Seguridad. Se realizará una validación de que la ST incluye toda la información descrita en el apartado anterior, que las hipótesis de entorno no contradicen las asociadas a la certificación que presenta el producto y que los requisitos de seguridad que son objeto de evaluación son los determinados por el CCN y que estos están planteados con claridad.

b) Etapa 2 – Instalación del producto. Para la instalación y configuración deberán tenerse en cuenta las guías asociadas a la certificación *Common Criteria* del producto. En este sentido, solamente será necesario considerar aquellos aspectos de configuración necesarios para evaluar las funcionalidades de seguridad incluidas en la evaluación complementaria. Por el contrario, en el caso de que haya aspectos de configuración no reflejados dentro de la guía *Common Criteria* que sean necesarios para evaluar las nuevas funcionalidades, se utilizarán guías complementarias proporcionadas por el fabricante o información pública.

c) Etapa 3 – Análisis de conformidad de la documentación aportada. El evaluador deberá comprobar que la información proporcionada cumple los requisitos relacionados con el contenido y la presentación, proporcionando

un veredicto sobre su completitud y legibilidad. Deberá indicar todas las no-conformidades existentes.

d) Etapa 4 – Análisis de conformidad – Pruebas Funcionales. Se seguirán las tareas descritas en la metodología LINCE.

e) Etapa 5 – Análisis de vulnerabilidades. Se seguirán las tareas descritas en la metodología LINCE. Dado que el producto presenta ya una certificación, el análisis de vulnerabilidades deberá centrarse en:

- Aquellas relacionadas con los requisitos incluidos en la DS.
- Aquellas vulnerabilidades públicas del producto publicadas con posterioridad a la certificación.

97. Para el análisis de la resistencia de los mecanismos y funciones se seguirán también las tareas descritas en la metodología LINCE.

f) Etapa 6 – Pruebas de penetración del TOE. Se seguirán las tareas descritas en la metodología LINCE. En el proceso de evaluación de un producto se deben realizar **pruebas de penetración** con el objetivo de confirmará la explotabilidad de las vulnerabilidades identificadas durante el análisis de vulnerabilidades. La duración de esta etapa será, por defecto, de **5 días laborables**. En caso de que el número de vulnerabilidades impida realizar esta etapa en este tiempo, el evaluador podrá justificarlo e incrementar el esfuerzo a su consideración.

E.4. VEREDICTO DE LA EVALUACIÓN

98. Se seguirá el proceso descrito en la metodología LINCE.

99. En casos extraordinarios, tras el correspondiente análisis de riesgos, podría cualificarse el producto/servicio con un CETR a FALLA.

E.5. RESULTADO DE LA EVALUACIÓN

100. Se seguirá el proceso descrito en la metodología LINCE.

ANEXO F. CUALIFICACIÓN DE SERIES DE PRODUCTOS

101. A lo largo de los procesos de cualificación del CPSTIC, en ocasiones, lo fabricantes presentan solicitudes asociadas a:

   a) Certificaciones que incluyen unos modelos/series de productos específicos.

   b) Modelos/series adicionales sobre los que corre el mismo *firmware* que el certificado y que, por diferentes motivos, no fueron incluidos en su día en la certificación.

102. El presente anexo pretende recoger la metodología de evaluación de los modelos/series descritos en el punto b).

F.1. TÉRMINOS Y DEFINICIONES

Serie de productos	Una serie de productos es un conjunto de productos de un desarrollador, construido sobre la misma base funcional, para abordar las mismas necesidades de seguridad. Sin embargo, su diseño, *hardware*, *firmware* o *software* pueden variar de un producto a otro. Estas diferencias pueden provenir de un *hardware* o plataforma subyacente diferente, o puede consistir en funciones adicionales debido a diferentes requisitos en el alcance o actuación.
TOE de referencia	Conjunto de modelos seleccionados en la certificación original aportada por el fabricante.
Modelos adicionales	Todos los modelos que no han sido incluidos en la certificación original aportada por el fabricante.
Desarrollador	Responsable del proceso de evaluación por parte del fabricante.

F.2. EVIDENCIAS ENTREGABLES NECESARIAS

103. El desarrollador deberá proporcionar las siguientes evidencias:

   a) Declaración de seguridad asociada a la certificación de partida. (Al cualificador y al evaluador).

   b) Guías de operación e instalación. (Al evaluador).

   c) Informe de análisis diferencial. (Al cualificador y al evaluador).

   d) Productos entregables. (Al evaluador).

F.2.1 GUÍAS DE OPERACIÓN E INSTALACIÓN

104. El desarrollador debe entregar las guías de operación e instalación asociadas a la certificación de partida (si aplica). Una vez que el evaluador haya seleccionado los

nuevos modelos objeto de evaluación, el desarrollador deberá realizar las actualizaciones necesarias para incluir dichos modelos en las guías.

F.2.2 INFORME DE ANÁLISIS DIFERENCIAL

105. El desarrollador debe elaborar el **Informe de Análisis Diferencial** (en adelante, IAD), que identificará las características compartidas y contendrá la descripción de las diferencias (*hardware*, *firmware* y *software*) entre los productos/series de productos adicionales que se pretendan cualificar y el TOE de referencia incluido en la certificación inicial.

106. A modo de resumen, se incluirá una representación matricial con las características de cada modelo, con objeto de facilitar de forma visual el grado de diferenciación entre unos modelos y otros.

107. Este IAD deberá estar firmado por el responsable técnico del desarrollador.

F.2.3 PRODUCTOS ENTREGABLES

108. El desarrollador debe proporcionar el **TOE de referencia** asociado a la certificación inicial, el resto de modelos adicionales que vayan a ser probados y el entorno de operación.

F.3. PROCEDIMIENTO DE EVALUACIÓN

109. Este capítulo establece el criterio de evaluación con el cual se verifican las funcionalidades de seguridad de los productos/series de productos adicionales.

F.3.1 PASO 0: VERIFICACIÓN DEL IAD

110. El evaluador verificará que el IAD está completo y es correcto desde un punto de vista formal. Es decir, se verificará que se incluyen todos los productos, las diferencias existentes entre ellos y su impacto en los requisitos de seguridad.

F.3.2 PASO 1: PLAN DE EVALUACIÓN

111. En base al IAD presentado por el fabricante y el TOE de referencia de la certificación de partida, el evaluador elaborará un plan de evaluación que incluirá:

a) Selección de los modelos sobre los que se realizarán pruebas.

b) Descripción de pruebas que es necesario realizar sobre cada uno de los modelos anteriormente seleccionados.

112. Este plan de pruebas deberá ser validado por el CCN.

113. Para la selección de modelos se utilizarán los siguientes criterios:

a) Modelos que presenten diferencias que puedan afectar a funcionalidades de seguridad certificadas. Se identificarán todos los modelos que presenten diferencias que puedan afectar a requisitos de seguridad incluidos en la Declaración de Seguridad de la certificación original. De entre ellos, se

seleccionará un subconjunto que implementen todas las diferencias detectadas. En caso de considerar dos (2) o más productos que presenten un conjunto de diferencias equivalentes, podrá seleccionarse un solo modelo representativo de toda la serie, salvo que el evaluador justifique la necesidad de repetir las pruebas en otro producto.

b) Modelos que no presenten diferencias que puedan afectar a funcionalidades de seguridad certificadas. Se seleccionará una muestra representativa. En caso de considerar series de productos, podrá seleccionarse un solo modelo representativo de toda la serie.

114. El evaluador, en base al IAD proporcionado por el desarrollador y la selección de los modelos descritos en el apartado anterior, elaborará un listado de pruebas necesarias con la justificación de las pruebas que es necesario realizar sobre cada uno de los modelos seleccionados.

115. Este listado deberá contener, como mínimo:

a) Pruebas de todas aquellas diferencias que afectan a funcionalidades de seguridad certificadas sobre los modelos seleccionados en el apartado anterior.

b) Pruebas de muestreo sobre los modelos seleccionados en el apartado anterior.

116. Además, especificará la carga de trabajo esperada para las pruebas funcionales, el análisis de vulnerabilidades y las pruebas de penetración.

F.3.3 PASO 2: EVALUACIÓN

117. El laboratorio de evaluación realiza las actividades definidas dentro del plan desarrollado en el paso 1.

118. El evaluador, de acuerdo al plan de pruebas, realizará las siguientes actividades:

a) Pruebas Funcionales.

b) Análisis de vulnerabilidades, sobre las funcionalidades de seguridad para las cuales se hayan detectado diferencias, en caso de existir.

c) Pruebas de penetración, sobre las funcionalidades de seguridad para las cuales se hayan detectado diferencias, en caso de existir.

F.4. RESTRICCIONES TEMPORALES Y DE ESFUERZO DE LA EVALUACIÓN

119. No se establecerán límites temporales para la realización de pruebas sobre aquellos modelos que presentan diferencias que puedan afectar a las funcionalidades de seguridad certificadas.

120. En caso de realizar muestreo, se establecerá un **esfuerzo mínimo de dos (2) días** sobre cada modelo de la muestra.

ANEXO G. CUALIFICACIÓN DE VERSIONES

121. A lo largo de los procesos de cualificación del CPSTIC, en ocasiones, los fabricantes presentan solicitudes asociadas a versiones de producto que no se corresponden a la versión certificada, ya que implementan cambios menores con respecto a esta.

122. En estos casos, aunque la versión considerada no cuenta con una certificación oficial, ya que esta se encuentra asociada unívocamente a una versión concreta, sí es posible basarse en esa certificación para poder cualificar la versión actual, siempre que se demuestre que estos cambios no afectan a funcionalidades de seguridad certificadas del producto o bien estos cambios pueden evaluarse en el contexto de una Evaluación STIC Complementaria (ANEXO E).

123. El presente anexo pretende recoger la metodología de evaluación de estas versiones que presentan cambios menores con respecto a una versión certificada.

G.1. EVIDENCIAS ENTREGABLES NECESARIAS

124. El desarrollador deberá proporcionar las siguientes evidencias:

a) Declaración de seguridad asociada a la certificación de partida. (Al cualificador y al evaluador).

b) Guías de operación e instalación. (Al evaluador).

c) Informe de análisis diferencial. (Al cualificador y al evaluador).

d) Productos entregables (nueva versión y entorno de operación). (Al evaluador).

G.1.1 GUÍAS DE OPERACIÓN E INSTALACIÓN

125. El desarrollador debe entregar las guías de operación e instalación asociadas a la certificación de partida (si aplica), con las actualizaciones necesarias según la nueva versión del producto.

G.1.2 INFORME DE ANÁLISIS DIFERENCIAL

126. El desarrollador debe elaborar el **Informe de Análisis Diferencial** (en adelante, IAD), que identificará las características compartidas y contendrá la descripción de las diferencias (*hardware*, *firmware* y *software*) entre la versión que se pretende cualificar y la incluida en la certificación inicial.

127. Este informe de análisis diferencial deberá estar firmado por el responsable técnico.

G.1.3 PRODUCTOS ENTREGABLES

128. El desarrollador debe proporcionar la nueva versión del producto, así como el entorno de operación en el que se realizará la evaluación.

G.2. PROCEDIMIENTO DE EVALUACIÓN

G.2.1 PASO 0: VERIFICACIÓN DEL IAD

129. El evaluador verificará que el IAD está completo y es correcto desde un punto de vista formal. Es decir, se verificará que se incluye una referencia a la nueva versión, las diferencias existentes entre ésta y la certificada y su impacto en los requisitos de seguridad.

G.2.2 PASO 1: PLAN DE EVALUACIÓN

130. En base al IAD presentado por el fabricante y la certificación de partida, el evaluador elaborará un plan de evaluación que incluirá un listado de las pruebas que es necesario realizar, junto con la justificación correspondiente.

131. Este listado deberá contener, como mínimo, pruebas de todas aquellas diferencias detectadas en la nueva versión que afecten a funcionalidades de seguridad certificadas.

132. Además, especificará la carga de trabajo esperada para las pruebas funcionales, el análisis de vulnerabilidades y las pruebas de penetración.

133. Este plan de pruebas deberá ser validado por el CPSTIC.

G.2.3 PASO 2: EVALUACIÓN

134. El laboratorio de evaluación realiza las actividades definidas dentro del plan desarrollado en el paso 1.

135. El evaluador, de acuerdo al plan de pruebas, realizará las siguientes actividades:

a) Pruebas Funcionales.

b) Análisis de vulnerabilidades, sobre las funcionalidades de seguridad para las cuales se hayan detectado diferencias, en caso de existir.

c) Pruebas de penetración, sobre las funcionalidades de seguridad para las cuales se hayan detectado diferencias, en caso de existir.

G.3. RESTRICCIONES TEMPORALES Y DE ESFUERZO DE LA EVALUACIÓN

136. No se establecerán límites temporales para la realización de las pruebas descritas en el Paso 2.

ANEXO H. EVALUACIONES STIC

137. Este anexo establece los pasos necesarios para la realización de Evaluaciones STIC basadas en la metodología LINCE (CCN-STIC-2001 y CCN-STIC-2002).

138. 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.

139. Este tipo de Evaluaciones se diferencian de las Evaluaciones STIC Complementarias en que son completas, es decir, se prueban todos los RFS, dado que el producto no presenta una certificación previa.

140. Se realizará una Evaluación STIC en los siguientes casos:

a) Servicios *cloud* que, por sus características, no son certificables según las metodologías existentes.

b) Productos *on premise* que se encuentran bajo el supuesto de excepcionalidad.

c) Otros casos en los que específicamente así lo requiera el CCN.

141. Las actividades realizadas en el contexto de la evaluación, los módulos considerados y el formato de DS, serán los mismos que para una evaluación LINCE, salvo en los siguientes puntos:

a) A diferencia de la evaluación LINCE, la Evaluación STIC no estará acotada en tiempo.

b) En el caso de tratarse de un servicio *cloud,* en el proceso de validación de la Declaración de Seguridad:

i. No será necesaria la identificación de la versión de servicio.

ii. No será necesaria la comprobación de que la Declaración de Seguridad incluye estrictamente todos los RFS de la taxonomía de productos declarada.

ANEXO I. CUALIFICACION DE PRODUCTOS EN CATEGORÍA ALTA A PARTIR DE UNA CERTIFICACIÓN LINCE

142. Como ya se indicó en el cuerpo de la presente guía, para la cualificación de un producto de seguridad puede recurrirse a una certificación Common Criteria o a una certificación LINCE.

143. Por norma general, a los productos candidatos a ser cualificados para Categoría ALTA del ENS se les exige una certificación Common Criteria, mientras que para Categoría MEDIA suele exigirse LINCE.

144. No obstante, un producto de seguridad podrá cualificarse para ENS Categoría ALTA partiendo de una certificación LINCE en vigor, siempre y cuando se aporten las siguientes evidencias:

    a) El producto se encuentra certificado LINCE. Esta certificación está en vigor y cubre los requisitos para Categoría MEDIA.

    b) La criptografía implementada por el producto y requerida en los RFS cumple los requisitos para Categoría ALTA.

    c) En el caso de que el conjunto de requisitos para Categoría ALTA sea mayor que para categoría MEDIA, deberá realizarse una Evaluación STIC complementaria, según define el ANEXO E, pero esta vez tomando como referencia una certificación LINCE en lugar de una Common Criteria.

    d) La actualización anual del análisis de vulnerabilidades y el test de penetración en un laboratorio acreditado. En el caso de que el producto se cualifique por primera vez, este requisito se validará mediante el contrato firmado con el laboratorio para la realización del mantenimiento el siguiente año. En este sentido, es importante destacar que este compromiso de actualización anual se realizará sobre la versión cualificada. En caso de que, además, se pretenda actualizar la versión, se realizará adicionalmente el proceso descrito en el ANEXO G.

145. En caso de que el producto deje de cumplir el apartado 144 a), éste será eliminado del CPSTIC.

146. En caso de que el producto deje de cumplir los apartados144 b) c) o d), este perderá la cualificación para Categoría ALTA y figurará como cualificado para Categoría MEDIA.

PUBLICACIONES DE DEFENSA

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