centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 106

Procedimiento de inclusión de productos y servicios de seguridad TIC en el CPSTIC



Octubre 2026

Edita:

Centro Criptológico Nacional, 2026

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.10.08 12:50:04 +02'00'

Fecha de Edición: Octubre de 2026

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
Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. INTRODUCCIÓN 3
2. OBJETO Y ALCANCE 5
3. TÉRMINOS Y DEFINICIONES 6
3.1 DEFINICIONES 6
3.2 ESTRUCTURA DEL CPSTIC 6
3.3 DOCUMENTOS DEL PROCEDIMIENTO DE INCLUSIÓN 7
4. PROCEDIMIENTO DE INCLUSIÓN EN EL LISTADO DE PRODUCTOS Y SERVICIOS CUALIFICADOS (CUALIFICACIÓN) 9
4.1 CUALIFICACIÓN INICIAL 11
4.1.1. PRODUCTOS DE SEGURIDAD TIC ON-PREMISE 11
4.1.2. PRODUCTOS DE SEGURIDAD TIC DESPLEGADOS EN NUBE 13
4.2 RENOVACIÓN DE LA CUALIFICACIÓN 13
4.3 AMPLIACIÓN DEL ALCANCE DE LA CUALIFICACIÓN (CUALIFICACIÓN DE NUEVAS VERSIONES SOFTWARE O MODELOS HARDWARE) 14
4.3.1. INCLUSIÓN DE NUEVAS VERSIONES 15
4.4 EXPEDIENTES Y PLAZOS DE CUALIFICACIÓN 15
4.4.1. APERTURA Y VIGENCIA DEL EXPEDIENTE 15
4.4.2. PLAZO DE RESOLUCIÓN DEL TRÁMITE 16
4.4.3. PRÓRROGA EXTRAORDINARIA 16
4.4.4. ARCHIVO DEL EXPEDIENTE Y NUEVA SOLICITUD 16
4.5 FASES DEL PROCEDIMIENTO 16
4.5.1. SOLICITUD DE INCLUSIÓN 16
4.5.2. REVISIÓN DE LA SOLICITUD Y COMUNICACIÓN DE INICIO DE EXPEDIENTE 20
4.5.3. REVISIÓN DE LA PROPUESTA DE DECLARACIÓN DE SEGURIDAD 20
4.5.4. REVISIÓN DE LA CERTIFICACIÓN O EVALUACIÓN APORTADA 21
4.5.5. INCLUSIÓN PROVISIONAL Y ENTREGA DEL PROCEDIMIENTO DE EMPLEO SEGURO 21
4.5.6. INCLUSIÓN DEFINITIVA 22
4.5.7. RENOVACIÓN O AMPLIACIÓN DEL ALCANCE 22
5. PROCEDIMIENTO DE INCLUSIÓN EN EL LISTADO DE CONFORMIDAD Y GOBERNANZA 23
5.1 SOLICITUD DE INCLUSIÓN 24
5.2 CONSIDERACIONES GENERALES 24
5.3 EVIDENCIAS REQUERIDAS 25
5.4 RESOLUCIÓN E INCLUSIÓN PROVISIONAL 25
5.5 RENOVACIÓN 26
5.6 RESUMEN DE EVIDENCIAS 26
6. VIGENCIA Y EXCLUSIÓN DE PRODUCTOS 26
6.1 VIGENCIA DE LA INCLUSIÓN DE PRODUCTOS EN EL CPSTIC 26
6.2 PRÓRROGA EXCEPCIONAL DE LA VIGENCIA 27
6.3 EXCLUSIÓN DEL CPSTIC 27
7. DISTINTIVOS DE INCLUSIÓN 28
7.1 CONDICIONES DE USO 28
7.2 DISTINTIVO DE PRODUCTO CUALIFICADO 28
7.3 DISTINTIVO DE PRODUCTO DE SEGURIDAD DESPLEGADO EN NUBE CUALIFICADO 29
7.4 DISTINTIVO DE CONFORMIDAD Y GOBERNANZA 29
8. REFERENCIAS 30
9. ABREVIATURAS 31

1. INTRODUCCIÓN

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.

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 Real Decreto 421/2004, de 12 de marzo [1], en sus artículos 1 y 2.1, que establecen 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.

Asimismo, el artículo 19, *Adquisición de productos de seguridad y contratación de servicios de seguridad*, del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) [2], establece:

> *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.*

Además, entre las medidas de seguridad detalladas en el anexo II del ENS para sistemas de información de categoría **MEDIA y ALTA**, se encuentran:

> – **[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 también 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 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.

En virtud de estas competencias, y para dar respuesta a lo previsto en el artículo 19 y en la medida [op.pl.5] del ENS, 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)** [3].

2. OBJETO Y ALCANCE

El objeto de la presente guía es definir el procedimiento y las evaluaciones requeridas para incluir un producto o servicio de seguridad en el CPSTIC [3], tanto en el listado de **Productos y Servicios Cualificados** como en el listado de Productos y Servicios para la **Conformidad y Gobernanza**. La inclusión en el listado de Productos Aprobados se rige por la CCN-STIC-102 [4] y queda fuera del alcance de esta guía.

La presente guía contiene tres anexos:

- Anexo A Plantilla de Justificación de Requisitos (JR),
- Anexo B Plantilla de Informe de Análisis Diferencial (IAD),
- Anexo C Plantilla de Procedimiento de Empleo Seguro (PES).

3. TÉRMINOS Y DEFINICIONES

3.1 DEFINICIONES

Producto de seguridad TIC on-premise: conjunto de componentes software, firmware y/o hardware que proporcionan funcionalidad de seguridad, diseñados para su uso o incorporación en un sistema o entorno operativo definido, y que se despliega y opera en la infraestructura del propio organismo.

Producto de seguridad TIC desplegado en nube: producto de seguridad que se suministra y opera sobre una infraestructura en la nube, en cualquiera de sus modalidades (SaaS, PaaS o IaaS).

Servicio de seguridad TIC: a efectos de la presente guía, el término "servicio" es equivalente al de "producto desplegado en nube".

Producto o servicio para la conformidad y gobernanza: aquel que, sin formar parte de la arquitectura de seguridad del sistema, facilita el cumplimiento de la normativa de seguridad y la gobernanza de la organización. Esta denominación abarca tanto los productos en formato on-premise como los productos de seguridad desplegados en nube.

Requisitos Fundamentales de Seguridad (RFS): requisitos mínimos de evaluación y/o certificación exigidos para que un determinado producto o servicio sea incluido en el CPSTIC. Estos requisitos vendrán determinados por diversos factores como el tipo de producto de seguridad, el caso de uso o el nivel de clasificación o categoría del ENS para el que se solicita la cualificación. Se encuentran definidos en la guía CCN-STIC-140 Taxonomía de referencia para productos de Seguridad TIC [5].

3.2 ESTRUCTURA DEL CPSTIC

El CPSTIC se estructura en tres (3) listados —Productos Aprobados, Productos y Servicios Cualificados y Conformidad y Gobernanza— definidos como sigue (véanse la Tabla 1 y la Figura 1):

a) **Productos y Servicios Aprobados**: productos y servicios que se consideran adecuados para el manejo de información clasificada de un determinado ámbito (nacional, Organismos Internacionales) y hasta un nivel de clasificación máximo especificado para cada producto.

b) **Productos y Servicios Cualificados**: productos y servicios de seguridad que cumplen los requisitos de seguridad exigidos por el CCN para el manejo de información sensible en el ENS. De forma análoga a lo que sucede con los productos y servicios aprobados, para cada producto o servicio se especificará la máxima categoría del sistema para el que se considera adecuado (ALTA o MEDIA).

c) **Productos y Servicios para la Conformidad y Gobernanza**: productos o servicios que, sin formar parte de la arquitectura de seguridad del sistema, facilitan el cumplimiento de la normativa de seguridad y la gobernanza de la seguridad.

Listado del CPSTIC	Información que maneja
Productos Aprobados	CLASIFICADA
Productos y Servicios Cualificados	SENSIBLE (ENS)
Conformidad y Gobernanza	Cualquier tipo

Tabla 1. Listados que componen el CPSTIC

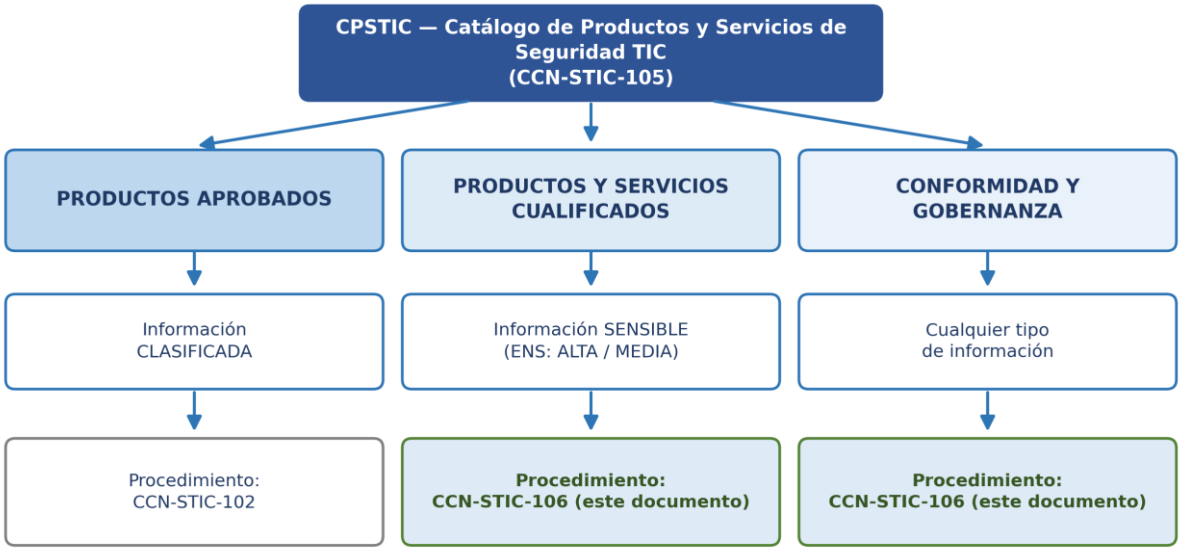


Figura 1. Estructura del CPSTIC y guías de procedimiento aplicables

Los RFS exigibles a los productos cualificados, en función del tipo de producto, se detallan en los anexos de la guía **CCN-STIC-140** [5].

Un producto cualificado por el CCN hará referencia a una configuración determinada y definida en un Procedimiento de Empleo Seguro (PES), que se publicará como una guía CCN-STIC que se referenciará en la información contenida en el CPSTIC.

3.3 DOCUMENTOS DEL PROCEDIMIENTO DE INCLUSIÓN

En el proceso de inclusión intervienen los documentos que se relacionan en la Tabla 2, en la que también se indica quién los elabora y la fuente que define su contenido.

Documento	Elabora	Contenido definido en
Solicitud de inclusión (FOR-CPSTIC-02) y declaración responsable (FOR-CPSTIC-01)	Solicitante	Formularios publicados en la web del CPSTIC
Declaración de Seguridad (DS) — Common Criteria o LINCE	Solicitante	Metodología de certificación de origen

Documento	Elabora	Contenido definido en
Declaración de Seguridad (DS) — Evaluación STIC Complementaria	Solicitante	CCN-STIC-2003 [6]
Declaración de Seguridad (DS) y Documento de Arquitectura del Servicio (DAS) — productos de seguridad desplegados en nube	Solicitante	Anexos A y B de la CCN-STIC-2010 [7] [8]
Justificación de Requisitos (JR)	Solicitante	Anexo A de la presente guía [9]
Informe de Análisis Diferencial (IAD)	Solicitante	Anexo B de la presente guía [10]
Procedimiento de Empleo Seguro (PES)	Solicitante	Anexo C de la presente guía [11]
Informe de pruebas de penetración — Conformidad y Gobernanza	Laboratorio acreditado en el ENECSTI	CCN-STIC 2030
Declaración responsable (DAS) — Conformidad y Gobernanza en nube	Solicitante	Anexo B de la CCN-STIC-2010
Plan de evaluación	Laboratorio	Validado por el CCN en cada expediente
Informes de evaluación (ITE, ITM)	Laboratorio	CCN-STIC-2004 [12] (ITE) y CCN-STIC-2010 [13] (ITM)
COM-INI, RRPDS, ITI y RITI	CCN	Apartado 4.5

Tabla 2. Documentos que intervienen en el procedimiento

La Figura 2 resume, para cada tipo de expediente, los trámites admitidos, la garantía exigida, las evidencias requeridas y la vigencia de la inclusión.

EXPEDIENTE DE CUALIFICACIÓN · Producto de seguridad TIC on-premise Apartado 4	
Trámites	Cualificación inicial · Renovación · Ampliación del alcance (series y versiones)
Garantía exigida	ALTA: Common Criteria, o LINCE con las condiciones del apartado 4.1.1.2 MEDIA: LINCE, como mínimo RFS no cubiertos: Evaluación STIC Complementaria (apartado 4.1.1.1)
Evidencias	Certificación CC/LINCE y DS (o propuesta de DS) · JR · política de versionado IAD en las ampliaciones del alcance
Vigencia	Expediente: hasta 5 años de antigüedad de la certificación Cualificación: 2 años o hasta el fin de soporte de seguridad, lo que ocurra antes

EXPEDIENTE DE CUALIFICACIÓN · Producto de seguridad desplegado en nube Apartado 4	
Trámites	Cualificación inicial · Renovación No admite ampliación del alcance: CICLON prescinde del versionado (4.3.1)
Garantía exigida	Evaluación CICLON (CCN-STIC-2010) que cubra los RFS de la familia y categoría Veredicto: Porcentaje de Garantía Compuesto (PGC = PGE + PGM)
Evidencias	DS y DAS (Anexos A y B de la CCN-STIC-2010) · JR
Vigencia	Expediente: coincide con la cualificación (2 años) Cualificación: 2 años · la renovación exige una nueva solicitud completa

EXPEDIENTE DE CONFORMIDAD Y GOBERNANZA Apartado 5	
Trámites	Inclusión · Renovación
Garantía exigida	Pruebas de penetración conforme a la CCN-STIC 2030, realizadas por un laboratorio acreditado en el ENECSTI
Evidencias	Informe de pruebas de penetración En nube, además: declaración responsable (DAS) de certificación ENS en vigor
Vigencia	Inclusión: 2 años · la renovación exige una nueva solicitud completa

Figura 2. Tipos de expediente y condiciones aplicables a cada listado

4. PROCEDIMIENTO DE INCLUSIÓN EN EL LISTADO DE PRODUCTOS Y SERVICIOS CUALIFICADOS (CUALIFICACIÓN)

Este apartado describe el procedimiento de inclusión en el listado de **Productos y Servicios Cualificados** del CPSTIC, aplicable tanto a los productos de seguridad TIC *on-premise* como a los productos de seguridad desplegados en nube. La Figura 3 representa *el* procedimiento.

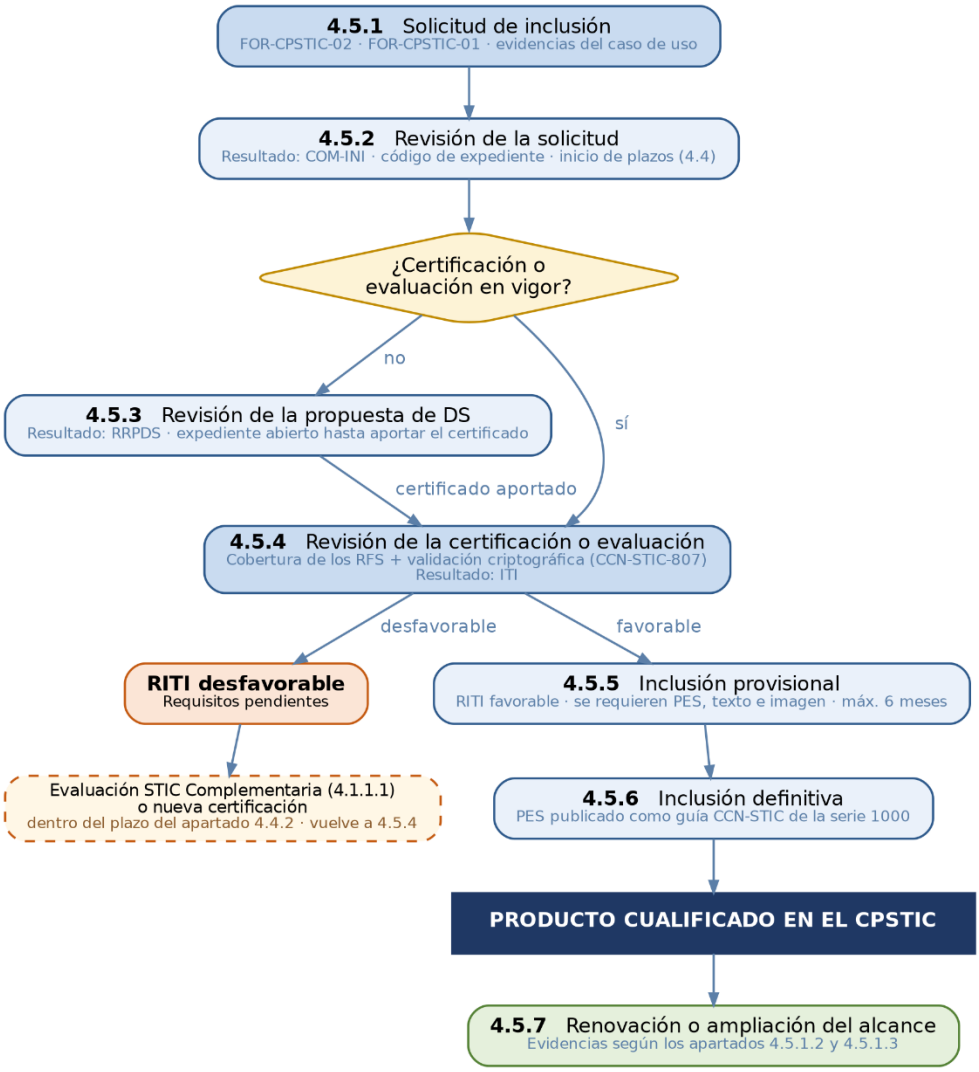


Figura 3. Procedimiento de inclusión en el listado de Productos y Servicios Cualificados

El solicitante deberá indicar en la solicitud de cualificación en qué familia o familias encaja el producto o servicio, de acuerdo con la taxonomía establecida en la guía CCN-STIC-140 [5], dado que de ellas dependen los RFS exigibles y las evidencias asociadas.

En caso de que el producto o servicio no encaje en ninguna familia de las contempladas en la taxonomía, el solicitante lo hará constar en la solicitud indicando la familia "Otras herramientas". El CCN estudiará individualmente dichas solicitudes y determinará, caso por caso, qué requisitos de seguridad deberá implementar y certificar el producto o servicio.

El CCN se reserva el derecho a:

a) Requerir información adicional para verificar que se han evaluado todos los RFS de la familia en aquellas solicitudes que aporten certificaciones.

b) No aceptar la solicitud en el caso de que no se solicite la cualificación de la funcionalidad principal del producto.

c) Requerir al solicitante información adicional sobre las funcionalidades de seguridad implementadas por el producto.

d) Revocar la cualificación de productos multifunción cuando el solicitante haga publicidad engañosa acerca de las funcionalidades cualificadas.

Dentro de este procedimiento se distinguen tres tipos de trámites:

a) Cualificación inicial.

b) Renovación de la cualificación.

c) Ampliación del alcance de la cualificación (cualificación de nuevas versiones software o modelos hardware).

4.1 CUALIFICACIÓN INICIAL

La cualificación inicial o inclusión en el listado de Productos y Servicios Cualificados exige acreditar una certificación o una evaluación reconocida por el CCN. En este apartado se definen los requisitos generales aplicables a cada tipo de producto.

4.1.1. PRODUCTOS DE SEGURIDAD TIC ON-PREMISE

Con carácter general, para que un producto sea cualificado para categoría **ALTA** del ENS deberá cumplir alguna de estas dos condiciones:

a) Poseer una certificación conforme a la metodología Common Criteria donde se incluyan los RFS definidos para esa familia o familias de productos.

b) Poseer una Certificación Nacional Esencial de Seguridad (LINCE) [14] donde se incluyan los RFS definidos para esa familia o familias de productos, siempre que se cumplan las condiciones adicionales descritas en el apartado 4.1.1.2.

Para la categoría MEDIA, el producto deberá contar, como mínimo, con una certificación **LINCE** [14].

En el caso de que la certificación aportada en cualquiera de los casos no incluya todos los RFS definidos para esa familia de productos, deberá completarse el proceso realizando una **Evaluación STIC Complementaria** como la descrita en el apartado 4.1.1.1.

4.1.1.1. EVALUACIÓN STIC COMPLEMENTARIA

En la Evaluación STIC Complementaria se incluirán los requisitos de seguridad no incluidos en la certificación inicial y deberá ser realizada, obligatoriamente, en uno de los laboratorios acreditados dentro del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI).

El procedimiento de evaluación estará basado en lo establecido en la metodología LINCE (CCN-STIC-2001 [14] y CCN-STIC-2002 [15]), aunque introducirá las siguientes modificaciones:

a) No existirán restricciones temporales.

b) El análisis de vulnerabilidades estará centrado en los requisitos incluidos en la DS y en las vulnerabilidades públicas posteriores a la certificación.

c) Las pruebas de penetración del objeto de evaluación (TOE) tendrán una duración mínima de **cinco días laborables**.

Para la realización de la Evaluación STIC Complementaria, el fabricante deberá aportar, como mínimo:

a) Declaración de Seguridad (DS).

b) Las guías de operación e instalación del TOE.

c) El entorno de ejecución.

La DS se elaborará conforme a la CCN-STIC 2003 [6] y deberá ser validada por el CCN antes del inicio de la evaluación. En ella se especificarán las funcionalidades de seguridad objeto de evaluación —las no cubiertas por la certificación de partida—, su correspondencia con los RFS pendientes y las hipótesis del entorno, que por defecto serán las de la certificación.

El resultado se recogerá en el Informe Técnico de Evaluación (**ITE**), elaborado conforme a la plantilla de la CCN-STIC-2004 [12].

4.1.1.2. CUALIFICACIÓN EN ENS ALTA A PARTIR DE UNA CERTIFICACIÓN LINCE

Los productos podrán cualificarse para **ENS ALTA partiendo de una certificación LINCE** en vigor, siempre que cumplan los siguientes requisitos:

a) La certificación LINCE está en vigor y cubre los requisitos para categoría MEDIA.

b) La criptografía implementada y requerida en los RFS cumple los requisitos para categoría ALTA.

c) Cuando el conjunto de requisitos exigidos para categoría ALTA sea mayor que para categoría MEDIA, se realizará una Evaluación STIC Complementaria (apartado 4.1.1.1), tomando como certificación de partida la certificación LINCE.

d) El producto se someterá de forma periódica, como mínimo una vez al año, a un análisis de vulnerabilidades y a pruebas de penetración en un laboratorio acreditado en el ENECSTI. En la primera cualificación, este compromiso se acreditará mediante el contrato firmado con el laboratorio para el mantenimiento del año siguiente; dicho mantenimiento se realizará sobre la versión cualificada. Adicionalmente, si se requiere actualizar la versión cualificada, se aplicará el procedimiento de ampliación del alcance descrito en el apartado 4.3.

Si el producto deja de cumplir la primera condición, será excluido del CPSTIC; si deja de cumplir cualquiera de las restantes, perderá la cualificación para ALTA y figurará como cualificado para categoría MEDIA. En particular, si el análisis de vulnerabilidades y las pruebas de penetración periódicos no cumplen los requisitos de categoría ALTA, el producto pasará a figurar como cualificado para categoría MEDIA; si el resultado es

desfavorable también frente a los requisitos de categoría MEDIA, el producto será excluido del CPSTIC.

4.1.2. PRODUCTOS DE SEGURIDAD TIC DESPLEGADOS EN NUBE

Para la cualificación de productos de seguridad desplegados en la nube, se exigirá una evaluación conforme a la Metodología de Evaluación de Productos en la Nube (**CICLON**) [13], descrita en la CCN-STIC-2010, donde se incluyan los RFS definidos para esa familia de producto en la categoría solicitada, conforme al apartado 4.5.1.

El veredicto de la evaluación CICLON es el **Porcentaje de Garantía Compuesto (PGC)**, que integra el Porcentaje de Garantía de Evaluación (PGE), obtenido en la fase de evaluación inicial, y el Porcentaje de Garantía de Monitorización (PGM), obtenido en la fase de monitorización continua y periódica. El PGC se actualiza en cada iteración de la fase de monitorización durante toda la vigencia de la certificación. Dependiendo del valor que tome el PGC, el producto podrá:

a) Ser incluido inicialmente como producto cualificado para categoría ALTA o MEDIA.

b) Mantenerse dentro del CPSTIC en la misma o diferente categoría.

c) Ser excluido del CPSTIC.

4.2 RENOVACIÓN DE LA CUALIFICACIÓN

Cuando un producto es incluido en el CPSTIC, se le asigna una “fecha de revisión de validez” que, como máximo, será de dos (2) años desde la cualificación inicial. Como su propio nombre indica, esta será la fecha en la que el solicitante y el equipo del CPSTIC deberán revisar si el producto puede o no continuar dentro del catálogo.

Para ello, el solicitante deberá garantizar las siguientes condiciones:

a) El producto, en la versión incluida en el CPSTIC, sigue teniendo soporte de seguridad, independientemente de si se sigue comercializando o no.

b) La certificación aportada para la cualificación tiene menos de cinco (5) años de antigüedad.

c) El producto sigue cumpliendo los RFS vigentes y no existen vulnerabilidades críticas no corregidas; para ello podrá requerirse una actualización del análisis de vulnerabilidades.

En caso de que se cumplan las tres condiciones, el fabricante remitirá al CPSTIC la correspondiente solicitud de renovación (FOR-CPSTIC-02); el CCN realizará las comprobaciones oportunas y actualizará la “fecha de revisión de validez” del producto.

Este procedimiento solamente se aplicará en el caso de los productos *on-premise*.

4.3 AMPLIACIÓN DEL ALCANCE DE LA CUALIFICACIÓN (CUALIFICACIÓN DE NUEVAS VERSIONES SOFTWARE O MODELOS HARDWARE)

Las metodologías de certificación Common Criteria y LINCE, utilizadas para la cualificación de productos *on-premise*, aplican únicamente a la versión o versiones del producto y los modelos hardware especificados en la DS asociada a la certificación.

Para la cualificación de versiones software posteriores a una certificada o modelos hardware no incluidos en la certificación inicial, se ha habilitado un procedimiento ágil que permite acreditar el cumplimiento de los RFS sin acometer un nuevo proceso de certificación, más costoso y prolongado y, en ocasiones, inviable atendiendo al ciclo de vida del producto.

Este procedimiento consiste en realizar una **Evaluación STIC Complementaria** como la descrita en el apartado 4.1.1.1, que incluya:

- **Nuevas versiones del producto.** Se evalúan las diferencias respecto a la versión certificada y, cuando la nueva versión introduzca funcionalidades de seguridad que afecten a los RFS, dichas funcionalidades.
- **Nuevos modelos o series de productos.** Se pretende extender la cualificación a otros modelos de la misma serie construidos sobre la misma base funcional. Se evalúan las diferencias de hardware, firmware y software respecto a los modelos certificados.

Para ambos casos, el CCN se reserva el derecho de no aplicar el procedimiento cuando se dé alguna de las siguientes circunstancias:

a) Los cambios detectados se consideran “cambios mayores” (p. ej.: afectan a la arquitectura del producto).

b) La certificación de partida tiene más de cinco (5) años de antigüedad.

La Tabla 3 recoge los términos empleados:

Serie de productos	Conjunto de productos de un desarrollador, construido sobre la misma base funcional, cuyo diseño, hardware, firmware o software puede variar de un producto a otro.
TOE de referencia	Conjunto de modelos seleccionados en la certificación original aportada por el fabricante.
Modelos adicionales	Modelos no incluidos en la certificación original que se pretenden cualificar.

Tabla 3. Términos empleados en la cualificación de series de productos

Para dar inicio al procedimiento, el solicitante deberá aportar:

a) La DS de la certificación de partida.

b) Un Informe **de Análisis Diferencial (IAD)**, conforme a la plantilla del Anexo B de la presente guía [10], firmado por el responsable técnico, con una matriz de características que describa las diferencias de *hardware*, *firmware* y *software* respecto al TOE de referencia. Cuando el producto haya sido objeto

de ampliaciones anteriores, el IAD podrá tomar como base el último IAD aceptado por el CCN, haciéndolo constar expresamente.

c) Opcionalmente, la propuesta de PES actualizada.

El procedimiento comprende: la verificación de la completitud del IAD y una Evaluación STIC Complementaria en caso de encontrar diferencias que impacten en las funcionalidades de seguridad requeridas. No se establecerán límites temporales para las pruebas sobre modelos con diferencias que afecten a funcionalidades de seguridad certificadas; en caso de muestreo, se establecerá un esfuerzo mínimo de dos (2) días por modelo.

4.3.1. INCLUSIÓN DE NUEVAS VERSIONES

Se aplica cuando se pretende cualificar una versión que no se corresponde con la certificada por implementar cambios, siempre que se demuestre que los cambios no afectan a funcionalidades de seguridad certificadas o que pueden evaluarse mediante esta evaluación. Cuando la nueva versión introduzca nuevas funcionalidades de seguridad que afecten a los RFS, la evaluación se aplicará sobre las funcionalidades añadidas.

Este procedimiento no se aplica a los productos de seguridad desplegados en nube, dado que la metodología CICLON prescinde del versionado e incorpora una fase de monitorización periódica que revisa de forma continuada el estado de seguridad del producto.

4.4 EXPEDIENTES Y PLAZOS DE CUALIFICACIÓN

El expediente es la unidad de tramitación que vincula un producto o servicio con su proceso de cualificación. Bajo un mismo expediente de cualificación se realizan todos los trámites relativos a un producto o servicio hasta el momento en que sea renovada su certificación.

4.4.1. APERTURA Y VIGENCIA DEL EXPEDIENTE

Una vez el CCN haya revisado la solicitud de cualificación y haya determinado que es correcta, remitirá al solicitante la **comunicación de inicio de expediente**, conforme a lo descrito en el apartado 4.5.2.

El expediente podrá permanecer abierto el tiempo en que se mantenga en vigor la certificación o evaluación que lo sustenta, es decir:

a) **Un máximo de cinco (5) años** en el caso de Common Criteria o LINCE.

b) **Un máximo de dos (2) años** en el caso de CICLON.

Durante este periodo, se tramitarán las solicitudes de renovación y de ampliación del alcance (nuevos modelos o versiones) referidas a esa certificación.

La obtención de una nueva certificación dará lugar a la apertura de un nuevo expediente y deberá solicitarse como inclusión inicial, aunque el producto ya figure en el catálogo.

En el caso de los productos *on-premise*, el expediente se cerrará cuando la certificación que lo sustenta alcance los cinco (5) años de antigüedad, momento en el que se dejarán de admitir renovaciones y ampliaciones del alcance.

En el caso de los productos de seguridad desplegados en nube, la vigencia del expediente coincide con la de la cualificación, por lo que cada inclusión da lugar a un nuevo expediente.

4.4.2. PLAZO DE RESOLUCIÓN DEL TRÁMITE

Cada trámite —inclusión inicial, renovación o ampliación del alcance— deberá resolverse en el plazo de **un (1) año** desde la emisión de la COM-INI correspondiente.

Durante ese periodo el solicitante deberá aportar las evidencias requeridas: el certificado, cuando se hubiera revisado una propuesta de declaración de seguridad (apartado 4.5.3), o el Informe Técnico de Evaluación (ITE), cuando se hubiera emitido un RITI desfavorable con requisitos pendientes (apartado 4.5.4). La revisión de versiones sucesivas de la propuesta de declaración de seguridad no reinicia el cómputo del plazo.

4.4.3. PRÓRROGA EXTRAORDINARIA

El plazo del apartado 4.4.2 podrá prorrogarse, **por una sola vez, seis (6) meses adicionales**, hasta un máximo de dieciocho (18) meses. La prórroga deberá solicitarse al CCN por escrito, de forma motivada y con anterioridad al vencimiento del plazo. Esta prórroga es independiente de la prórroga excepcional de la vigencia prevista en el apartado 6.2, que se refiere a productos ya incluidos en el catálogo.

4.4.4. ARCHIVO DEL EXPEDIENTE Y NUEVA SOLICITUD

Transcurrido el plazo, con su prórroga en su caso, sin que se hayan aportado las evidencias requeridas, el expediente se **archivará**. Una nueva solicitud se tramitará desde el inicio, verificándose los RFS de la familia y los algoritmos criptográficos autorizados que se encuentren vigentes en ese momento.

4.5 FASES DEL PROCEDIMIENTO

El procedimiento se estructura en las fases descritas en este apartado. La solicitud y su revisión son comunes a todos los casos de uso; las restantes fases se aplican en función del caso de uso solicitado, conforme a la Tabla 4.

4.5.1. SOLICITUD DE INCLUSIÓN

Documentos de entrada: los formularios FOR-CPSTIC-02 y FOR-CPSTIC-01 y las evidencias exigibles al caso de uso declarado, que se detallan en los apartados 4.5.1.1 a 4.5.1.3.

Con independencia de la modalidad, el proceso se inicia con el envío al CCN (soporte.cpstic@ccn.cni.es) de la **solicitud de inclusión** en el listado de Productos y

Servicios Cualificados, cumplimentando los siguientes formularios, disponibles en la web del CPSTIC (https://cpstic.ccn.cni.es):

- **FOR-CPSTIC-02** — Solicitud de inclusión en el Catálogo de Productos y Servicios STIC (CPSTIC).
- **FOR-CPSTIC-01** — Declaración responsable para la inclusión en el Catálogo de Productos y Servicios STIC (CPSTIC).

La solicitud podrá presentarla el fabricante, un suministrador o un organismo de la Administración.

4.5.1.1. CUALIFICACIÓN INICIAL

Aplicable cuando se pretende incluir por primera vez un producto y una versión concretos en el CPSTIC, o cuando se ha obtenido una nueva certificación que da lugar a la apertura de un nuevo expediente (apartado 4.4.1). Según lo declarado en la solicitud se aportará:

Producto de seguridad TIC on-premise con certificación en vigor. Junto a la solicitud se adjuntará:

a) La **certificación *Common Criteria* o LINCE** y su **Declaración de Seguridad (DS)**.

b) **Justificación de Requisitos (JR)**, conforme a la plantilla del Anexo A de la presente guía [9], siempre y cuando existan diferencias entre los RFS definidos para la familia solicitada y los declarados en la declaración de seguridad.

c) **Informe de Análisis Diferencial (IAD)**, conforme a la plantilla del Anexo B de la presente guía [10], cuando la versión o los modelos que se pretenden cualificar no coincidan con los recogidos en la certificación aportada.

d) Opcionalmente, la **política de versionado** del producto, que describa el significado de cada carácter de la versión y las condiciones de actualización.

e) Opcionalmente, el listado de algoritmos criptográficos empleados y una propuesta de PES (obligatoria una vez incluido el producto) conforme a la plantilla del Anexo C de la presente guía [11].

Producto de seguridad TIC on-premise sin certificación en vigor. El producto aún no dispone de certificación Common Criteria o LINCE y pretende certificarse. Junto a la solicitud se adjuntará:

a) La **propuesta de Declaración de Seguridad (DS)** con la que se pretende certificar el producto, que el CCN revisará conforme al apartado 4.5.3.

b) La **Justificación de Requisitos (JR)**, conforme a la plantilla del Anexo A de la presente guía [9].

c) La **política de versionado** del producto, que describa el significado de cada carácter de la versión y las condiciones de actualización.

d) Opcionalmente, el listado de algoritmos criptográficos empleados y una propuesta de PES (obligatoria una vez incluido el producto) conforme a la plantilla del Anexo C de la presente guía [11].

Emitido el RRPDS, el expediente permanecerá abierto hasta que el solicitante aporte el certificado, dentro del plazo del apartado 4.4.2. Aportado el certificado, el procedimiento continúa por la fase de revisión de la certificación (apartado 4.5.4).

Producto de seguridad desplegado en nube. El producto deberá cumplir los RFS asociados a su funcionalidad principal (los mismos que un producto de seguridad TIC on-premise equivalente). Los requisitos genéricos aplicables a cualquier producto de seguridad desplegado en nube quedan cubiertos por la propia metodología CICLON durante la evaluación y la monitorización.

Junto a la solicitud se adjuntará:

a) La **Declaración de Seguridad (DS)**, conforme a la plantilla del **Anexo A de la CCN-STIC-2010** [7], que será validada en primera instancia por el equipo del CPSTIC.

b) El **Documento de Arquitectura del Servicio (DAS)**, conforme a la plantilla del **Anexo B de la CCN-STIC-2010** [8], que recoge la estructura del TOE y su entorno operativo, los flujos de información, la jurisdicción de los datos y el cumplimiento de los requisitos de transparencia, entre otros aspectos.

c) La **Justificación de Requisitos (JR),** conforme a la plantilla del Anexo A de la presente guía [9].

d) Opcionalmente, el listado de algoritmos criptográficos empleados y una propuesta de PES (obligatoria una vez incluido el producto).

4.5.1.2. RENOVACIÓN

Aplicable cuando el producto ya está incluido en el CPSTIC y se pretende mantener su cualificación una vez próxima o alcanzada la fecha de revisión de validez.

Productos de seguridad TIC on-premise. A tal efecto, bastará con presentar la solicitud (FOR-CPSTIC-02) marcando la opción de **renovación** y aportar la evidencia de que el producto mantiene soporte de seguridad: un documento firmado por el fabricante cuando dicha información no sea pública o, cuando lo sea, un informe con la captura de pantalla de la evidencia y la URL de la página o del documento público.

Productos de seguridad desplegados en nube. La renovación exige una **nueva solicitud completa**, aportando toda la información y las evidencias como si se tratara de una inclusión inicial (apartado 4.5.1.1), y dará lugar a una nueva evaluación CICLON. Alcanzada la fecha de vigencia sin renovación, el producto será excluido del CPSTIC (apartado 6.3).

4.5.1.3. AMPLIACIÓN DEL ALCANCE

Aplicable cuando se pretende ampliar el alcance de la cualificación a una nueva versión del producto o a nuevos modelos o *appliances* de una serie, partiendo de la certificación

y de la cualificación existentes. La ampliación actualiza la fecha de la revisión de la cualificación (apartado 6.1).

Según lo declarado en la solicitud, la ampliación podrá referirse a **series de productos** o a **versiones**. En ambos casos se aportará:

a) La **Declaración de Seguridad** de la certificación de partida.

b) El **Informe de Análisis Diferencial (IAD)**, conforme a la plantilla del Anexo B de la presente guía Cuando el producto haya sido objeto de ampliaciones anteriores, el IAD podrá tomar como base el último IAD aceptado por el CCN, haciéndolo constar expresamente. [10].

c) Opcionalmente, la propuesta de PES actualizada.

El CCN revisará el IAD y validará qué funciones de seguridad deben ser nuevamente evaluadas o certificadas. Si no procede evaluar ninguna función adicional, el expediente avanzará hasta la inclusión del producto en el catálogo. Si, por el contrario, es necesario evaluar funciones de seguridad adicionales, el solicitante podrá optar entre una **Evaluación STIC Complementaria** (apartado 4.1.1.1) o una **nueva certificación** Common Criteria o LINCE.

4.5.1.4. RESUMEN DE EVIDENCIAS POR CASO DE USO

La Tabla 4 resume, para cada caso de uso, la documentación a aportar y las fases y evaluación aplicables.

Caso de uso	Documentación a aportar	Fases y evaluación aplicables
Inclusión inicial · on-premise con certificación en vigor	Solicitud (FOR-CPSTIC-02/01), certificación CC/LINCE y DS, JR (según caso) y política de versionado (opcional).	Fases 4.5.1 · 4.5.2 · 4.5.4 · 4.5.5 · 4.5.6. Revisión de la certificación frente a los RFS; si no los cubre en su totalidad, Evaluación STIC Complementaria (4.1.1.1).
Inclusión inicial · on-premise sin certificación en vigor	Solicitud, propuesta de DS y JR.	Fases 4.5.1 · 4.5.2 · 4.5.3 · 4.5.4 · 4.5.5 · 4.5.6. Revisión de la propuesta de DS (RRPDS); aportado el certificado, se revisa conforme al apartado 4.5.4.
Inclusión inicial · producto de seguridad desplegado en nube	Solicitud, DS y DAS (Anexos A y B de la CCN-STIC-2010) y JR.	Fases 4.5.1 · 4.5.2 · 4.5.3 · 4.5.4 · 4.5.5 · 4.5.6. Evaluación CICLON; veredicto PGC (4.1.2).
Renovación · on-premise	Solicitud (FOR-CPSTIC-02) y evidencia de soporte de seguridad vigente; en su caso, actualización del análisis de vulnerabilidades.	Fases 4.5.1 · 4.5.2 · 4.5.4 · 4.5.7. Verificación de certificación en vigor (menos de 5 años) y de soporte de seguridad; renueva 2 años o hasta el fin de soporte, lo que ocurra antes.
Renovación · producto de seguridad desplegado en nube	Solicitud y evidencias completas, como una inclusión inicial.	Fases 4.5.1 · 4.5.2 · 4.5.3 · 4.5.4 · 4.5.5 · 4.5.6. Nueva evaluación CICLON.

Caso de uso	Documentación a aportar	Fases y evaluación aplicables
Ampliación del alcance · series de productos	Solicitud, DS de partida, IAD con matriz de características y, opcionalmente, PES actualizado.	Fases 4.5.1 · 4.5.2 · 4.5.4 · 4.5.7. Evaluación STIC Complementaria (4.1.1.1): plan de evaluación validado por el CCN y muestreo (mínimo 2 días por modelo).
Ampliación del alcance · versiones	Solicitud, DS de partida, IAD y, opcionalmente, PES actualizado.	Fases 4.5.1 · 4.5.2 · 4.5.4 · 4.5.7. Evaluación STIC Complementaria (4.1.1.1) sobre las diferencias que afecten a funcionalidades de seguridad certificadas.
Supuesto · ENS ALTA con certificación LINCE (adicional a la inclusión inicial)	Además de lo exigido en la inclusión inicial: certificación LINCE en vigor para categoría MEDIA y contrato con laboratorio para el mantenimiento anual.	Condiciones del apartado 4.1.1.2: criptografía de categoría ALTA; si los RFS de ALTA exceden los de MEDIA, Evaluación STIC Complementaria; análisis de vulnerabilidades y pruebas de penetración al menos anuales.

Tabla 4. Resumen de evidencias, fases y evaluación por caso de uso

4.5.2. REVISIÓN DE LA SOLICITUD Y COMUNICACIÓN DE INICIO DE EXPEDIENTE

Documentos de entrada: ninguno adicional; en su caso, la subsanación de los defectos de forma que el CCN requiera.

Revisada la solicitud y subsanado cualquier defecto de forma, el CCN notificará el inicio del procedimiento mediante la **comunicación de inicio de expediente (COM-INI)**, que asignará un código de expediente y determinará el cómputo de los plazos previstos en el apartado 4.4. A continuación, el personal del CCN revisará la documentación y las evidencias aportadas.

Resultado: comunicación de inicio de expediente (COM-INI), que asigna el código de expediente y determina el cómputo de los plazos del apartado 4.4.

4.5.3. REVISIÓN DE LA PROPUESTA DE DECLARACIÓN DE SEGURIDAD

Esta fase solo resulta aplicable a los productos que no dispongan de una certificación en vigor, tanto de seguridad TIC *on-premise* como desplegados en nube.

Documentos de entrada: la propuesta de Declaración de Seguridad y la Justificación de Requisitos (apartado 4.5.1.1) y, dentro del plazo del apartado 4.4.2, el certificado emitido.

El CCN analizará la propuesta de declaración de seguridad y la Justificación de Requisitos frente a los RFS de la familia y la categoría declaradas, y emitirá el **resultado de la revisión de la propuesta de declaración de seguridad (RRPDS)**, que indicará si, una vez el producto se certifique conforme a dicha declaración de seguridad, cumplirá los requisitos exigidos por el catálogo. De este modo el solicitante conoce de antemano el resultado esperado antes de invertir en la certificación, y evita que una certificación ya emitida obligue después a una Evaluación STIC Complementaria o a un nuevo proceso de certificación.

El expediente permanecerá abierto, en los términos del apartado 4.4, hasta que el solicitante aporte el certificado emitido. Durante ese periodo el solicitante podrá requerir al CCN la revisión de versiones sucesivas de la propuesta de declaración de seguridad. Aportado el certificado, el procedimiento continúa por la fase de revisión de la certificación (apartado 4.5.4), tanto si la certificación se ha emitido sobre la declaración de seguridad revisada como sobre una distinta.

Resultado: resultado de la revisión de la propuesta de declaración de seguridad (RRPDS).

4.5.4. REVISIÓN DE LA CERTIFICACIÓN O EVALUACIÓN APORTADA

Documentos de entrada: la certificación Common Criteria o LINCE, o el informe de la evaluación CICLON, el listado de algoritmos criptográficos empleados y las evidencias complementarias que el CCN requiera.

El CCN verifica en esta fase que la certificación o la evaluación aportada cubre los RFS de la familia y la categoría solicitadas.

Productos de seguridad TIC on-premise. Si la certificación Common Criteria o LINCE cubre todos los RFS exigibles, el CCN realizará una revisión básica, sin evaluaciones adicionales en laboratorio, y emitirá un ITI FAVORABLE con la propuesta de inclusión y comunicará al solicitante el Resultado del Informe Técnico de Inclusión (RITI) FAVORABLE.

Si la certificación no cubre todos los RFS, el CCN emitirá un **RITI DESFAVORABLE** en el que indicará los requisitos pendientes, que el solicitante podrá acreditar mediante una Evaluación STIC Complementaria (apartado 4.1.1.1) o mediante una nueva certificación conforme a los requisitos exigidos, dentro del plazo previsto en el apartado 4.4.2.

Cuando el RITI sea DESFAVORABLE, indicará el grado de cumplimiento de los RFS y las evaluaciones o pruebas complementarias requeridas.

Productos de seguridad desplegados en nube. El CCN verificará el resultado de la evaluación CICLON en los términos del apartado 4.1.2.

De forma simultánea, si el producto emplea algoritmos criptográficos, el CCN validará que presentan la seguridad criptológica requerida y que se encuentran entre los autorizados para el ENS (CCN-STIC-807 [16]), según la categoría solicitada.

Resultado: Informe Técnico de Inclusión (ITI), que incorpora la validación criptográfica, y comunicación del RITI. Cuando el resultado sea desfavorable, el CCN emitirá un RITI DESFAVORABLE indicando los requisitos pendientes.

4.5.5. INCLUSIÓN PROVISIONAL Y ENTREGA DEL PROCEDIMIENTO DE EMPLEO SEGURO

Documentos de entrada: el Informe Técnico de Inclusión (ITI) favorable emitido en la fase anterior, el RITI FAVORABLE comunicado en la fase anterior y la descripción y la imagen del producto aportadas por el solicitante.

Comunicado el RITI FAVORABLE, el solicitante aportará la descripción y la imagen del producto para su ficha en el catálogo y, si no lo hubiera aportado con la solicitud, el Procedimiento de Empleo Seguro (PES).

Recibidas la descripción y la imagen, el CCN incluirá el producto en el listado de Productos y Servicios Cualificados como **Cualificado**, con carácter **provisional** hasta la entrega del PES. El periodo provisional tendrá una duración máxima de **seis (6) meses**. El PES se elaborará conforme a la plantilla del Anexo C de la presente guía [11].

La propuesta se remitirá, en formato editable y respetando la estructura y los estilos de dicha plantilla, a la dirección soporte.cpstic@ccn.cni.es, indicando en el asunto el nombre del producto y el código de expediente.

El Anexo C se publica en formato PDF; su versión editable puede solicitarse a través de la misma dirección.

Cuando el producto vaya a ser además aprobado para el manejo de información nacional clasificada conforme a la CCN-STIC-102, el PES cubrirá el caso de uso recogido a tal efecto en el Anexo C.

El producto se considerará cualificado desde la notificación del RITI favorable, aunque por motivos editoriales no figure todavía en el catálogo.

Resultado: inclusión provisional del producto en el CPSTIC. La provisionalidad decae con la entrega del PES, en el plazo máximo de seis (6) meses.

4.5.6. INCLUSIÓN DEFINITIVA

Documentos de entrada: el Procedimiento de Empleo Seguro (PES) entregado conforme al apartado 4.5.5.

El CCN revisará el PES aportado y podrá devolverlo con comentarios; el solicitante remitirá las versiones corregidas por el mismo canal hasta obtener la conformidad del CCN. Una vez validado, el CCN lo publicará como guía CCN-STIC de la serie 1000.

Publicada la guía, el producto dejará de figurar con carácter provisional y quedará incluido de forma **definitiva** en el listado, durante el periodo que corresponda, de acuerdo con el apartado 6.1.

Toda ampliación del alcance o nueva versión cualificada que afecte al contenido del PES obligará al solicitante a remitir una versión actualizada por el mismo canal, que dará lugar a una nueva edición de la guía.

Resultado: publicación del PES como guía CCN-STIC de la serie 1000 e inclusión definitiva del producto en el CPSTIC.

4.5.7. RENOVACIÓN O AMPLIACIÓN DEL ALCANCE

Documentos de entrada: la solicitud de renovación o de ampliación del alcance y las evidencias exigibles conforme a los apartados 4.5.1.2 y 4.5.1.3, según corresponda.

Realizadas las comprobaciones que se describen a continuación, el CCN actualizará la fecha de revisión de validez y renovará la cualificación por **dos (2) años o hasta la fecha**

de fin de soporte de seguridad declarada por el fabricante, lo que ocurra antes, y dentro del límite máximo de cinco (5) años de antigüedad de la certificación.

El procedimiento es el siguiente:

a) Con antelación suficiente al vencimiento, el fabricante remite la solicitud (FOR-CPSTIC-02) indicando la modalidad: renovación de la cualificación o ampliación del alcance.

b) Aporta la **evidencia de soporte de seguridad** vigente (por ejemplo, el ciclo de vida o el comunicado de soporte del fabricante) y, en el caso de una ampliación, el Informe de Análisis Diferencial (IAD).

c) El CCN verifica que la certificación (CC/LINCE) tiene una antigüedad inferior a cinco (5) años y que se mantiene el soporte de seguridad.

d) Superada la verificación y, en su caso, las pruebas asociadas a la ampliación, el CCN amplía la vigencia por dos (2) años o hasta la fecha de fin de soporte declarada, lo que ocurra antes.

e) Si existe una Evaluación STIC Complementaria o una certificación en curso, se aplicará la prórroga excepcional de tres (3) meses (apartado 6.2).

Alcanzada la fecha de revisión de validez sin que se produzca la renovación o la ampliación, el producto será excluido del CPSTIC conforme al apartado 6.3.

Resultado: renovación o ampliación del alcance de la cualificación.

5. PROCEDIMIENTO DE INCLUSIÓN EN EL LISTADO DE CONFORMIDAD Y GOBERNANZA

Este apartado describe el procedimiento de inclusión en el listado de Conformidad y Gobernanza. La *Figura 4* lo representa.

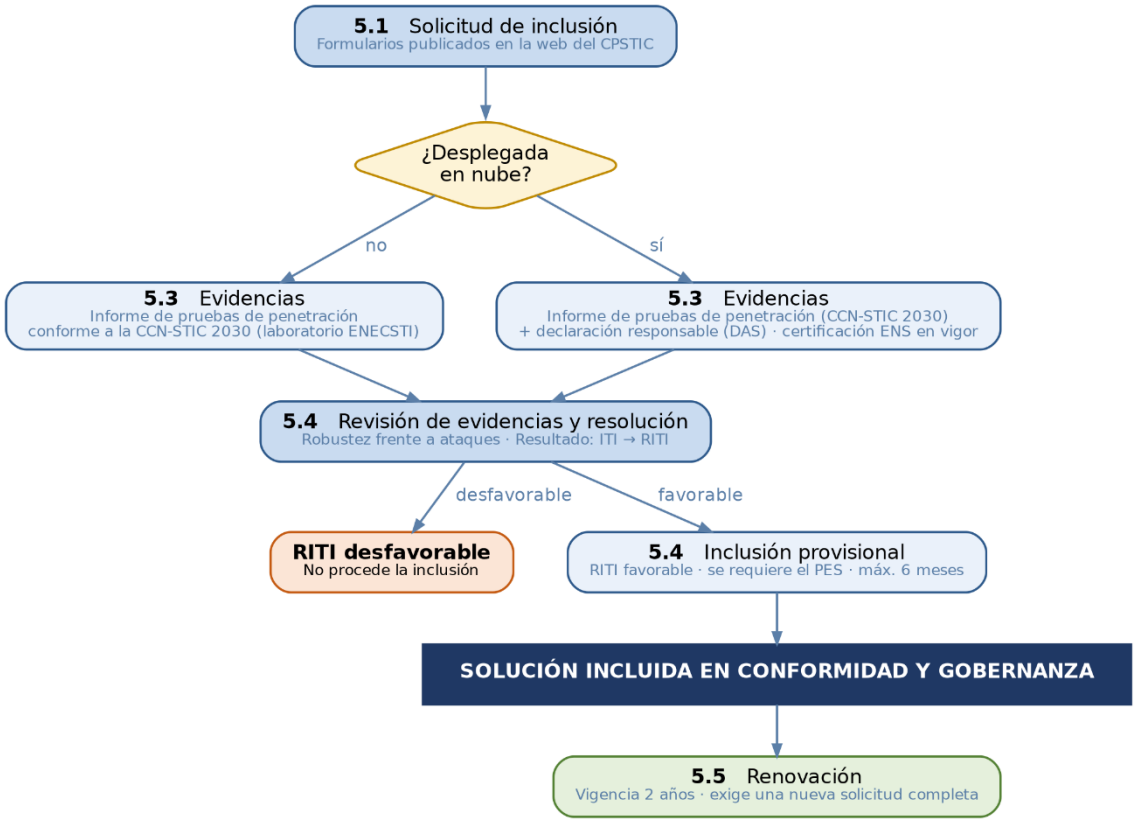


Figura 4. Procedimiento de inclusión en el listado de Conformidad y Gobernanza

5.1 SOLICITUD DE INCLUSIÓN

El proceso se inicia con el envío al CCN (soporte.cpstic@ccn.cni.es) de la **solicitud de inclusión** en el listado de Conformidad y Gobernanza, cumplimentando los formularios de solicitud publicados en la web del CPSTIC (https://cpstic.ccn.cni.es).

La solicitud podrá presentarla el fabricante, un suministrador o un organismo de la Administración.

Las evidencias que deben acompañar a la solicitud se detallan en el apartado 5.3.

5.2 CONSIDERACIONES GENERALES

El listado de **Conformidad y Gobernanza** agrupa soluciones que, sin formar parte de la arquitectura de seguridad del sistema, facilitan el cumplimiento de la normativa de seguridad y la gobernanza de la seguridad. Por su naturaleza, pueden emplearse en sistemas que manejen cualquier tipo de información.

Al no formar parte de la arquitectura de seguridad, estas soluciones **no disponen de RFS asociados en la CCN-STIC-140** [5]. En consecuencia, su inclusión no se sustenta en la verificación del cumplimiento de RFS, sino en la comprobación de la robustez de la solución frente a ataques, en los términos del apartado 5.3.

A título orientativo, entre las categorías de soluciones susceptibles de figurar en este listado se encuentran las herramientas de gobierno, riesgo y cumplimiento (GRC), las de apoyo al cumplimiento del ENS o del RGPD, las de concienciación y formación en seguridad, las de identificación remota por vídeo o las de gestión de vulnerabilidades, entre otras.

5.3 EVIDENCIAS REQUERIDAS

Junto a la solicitud de inclusión (apartado 5.1), y según el tipo de solución, se aportará la documentación siguiente.

Soluciones no desplegadas en nube. Deberán aportar un informe de pruebas de penetración, elaborado por un laboratorio acreditado en el ENECSTI, que verifique su resistencia frente a las pruebas descritas en la guía CCN-STIC 2030 Metodología de evaluación de seguridad en entornos web [17]. El informe contendrá, como mínimo:

- La identificación inequívoca de la solución evaluada, su versión y el entorno de pruebas.
- Las vulnerabilidades detectadas, su criticidad y su explotabilidad.
- El veredicto: la existencia de vulnerabilidades críticas o de vulnerabilidades explotables no subsanadas dará lugar a un resultado desfavorable.

Productos de seguridad desplegados en nube. Deberán aportar el informe de pruebas de penetración en los mismos términos que las soluciones no desplegadas en nube y, **además**, como única evidencia documental adicional, una declaración responsable basada en la plantilla del **Anexo B de la CCN-STIC-2010** [8] (Documento de Arquitectura del Servicio, DAS), en la que se acredite que el sistema o los sistemas sobre los que se despliega el producto disponen de una **certificación de conformidad con el ENS en vigor**.

5.4 RESOLUCIÓN E INCLUSIÓN PROVISIONAL

El CCN revisará la documentación y las evidencias aportadas y elaborará el **Informe Técnico de Inclusión (ITI)**, cuyo resultado comunicará mediante el **Resultado del Informe Técnico de Inclusión (RITI)**, que podrá ser FAVORABLE o DESFAVORABLE.

Si el RITI es favorable, el CCN incluirá la solución en el listado de Conformidad y Gobernanza, con carácter **provisional** hasta la entrega del Procedimiento de Empleo Seguro (PES), si no se hubiera aportado con la solicitud. El periodo provisional tendrá una duración máxima de **seis (6) meses**. El PES se elaborará conforme a la plantilla del Anexo C de la presente guía [11]. En caso de que el PES no sea aplicable, la solución se incluirá de forma definitiva.

La propuesta se remitirá en los mismos términos previstos en el apartado 4.5.5.

Incluida la solución en el listado, podrá emplear el distintivo de Conformidad y Gobernanza (apartado 7.4).

5.5 RENOVACIÓN

La inclusión en el listado de Conformidad y Gobernanza, tanto si la solución es *on-premise* como si es un producto de seguridad desplegado en nube, tiene una **vigencia de dos (2) años**. **La renovación exige una nueva solicitud**, aportando toda la información y las evidencias como si se tratara de una nueva inclusión. Conforme al apartado 6.2, la validez podrá prorrogarse excepcionalmente tres (3) meses cuando existan unas pruebas de penetración en curso.

5.6 RESUMEN DE EVIDENCIAS

La Tabla 5 resume las evidencias requeridas para la inclusión en el listado de Conformidad y Gobernanza.

Evidencias requeridas para la inclusión en el listado de Conformidad y Gobernanza	
Tipo de solución	**Evidencias y evaluación exigidas**
Solución no desplegada en nube	Informe de pruebas de penetración conforme a la CCN-STIC 2030, realizado por un laboratorio acreditado en el ENECSTI.
Producto de seguridad desplegado en nube	Informe de pruebas de penetración conforme a la CCN-STIC 2030, realizado por un laboratorio acreditado en el ENECSTI; y declaración responsable basada en la plantilla del Anexo B de la CCN-STIC-2010 (DAS) que acredite que el sistema o los sistemas sobre los que se despliega el producto disponen de certificación de conformidad con el ENS en vigor.

Tabla 5. Evidencias requeridas para la inclusión en Conformidad y Gobernanza

6. VIGENCIA Y EXCLUSIÓN DE PRODUCTOS

Este apartado desarrolla las condiciones de vigencia de la inclusión en el CPSTIC, la prórroga excepcional aplicable a los productos ya incluidos y los motivos de exclusión del catálogo.

6.1 VIGENCIA DE LA INCLUSIÓN DE PRODUCTOS EN EL CPSTIC

La inclusión en el CPSTIC, en cualquiera de los listados objeto de esta guía, tiene una **vigencia de dos (2) años**. Las particularidades de la renovación y, en su caso, de la ampliación de la vigencia se detallan en los apartados 4.5.1.2, 4.5.7 y 5.5. La Tabla 6 resume dichas condiciones.

Listado	Vigencia	Renovación / ampliación
Productos de seguridad cualificados (on-premise)	2 años o hasta el fin de soporte de seguridad declarado por el fabricante (lo que ocurra antes)	Puede renovarse o ampliarse si el producto mantiene soporte de seguridad (con evidencia) y la certificación (CC/LINCE) tiene menos de 5 años.

Listado	Vigencia	Renovación / ampliación
Productos de seguridad desplegados en nube	2 años	La renovación exige una nueva solicitud, aportando toda la información como si fuera una nueva inclusión.
Conformidad y Gobernanza (on-premise o nube)	2 años	La renovación exige una nueva solicitud, aportando toda la información como si fuera una nueva inclusión.

Tabla 6. Vigencia de la inclusión en el CPSTIC por listado

6.2 PRÓRROGA EXCEPCIONAL DE LA VIGENCIA

Para los listados de Productos y Servicios Cualificados y de Conformidad y Gobernanza, la validez de la inclusión podrá ampliarse excepcionalmente **tres (3) meses adicionales** cuando el fabricante haya iniciado un proceso de inclusión o de renovación que requiera una Evaluación STIC Complementaria, una certificación o, en el caso de las soluciones de Conformidad y Gobernanza, unas pruebas de penetración, con el fin de dar tiempo a que dicho proceso finalice.

6.3 EXCLUSIÓN DEL CPSTIC

Un producto, producto de seguridad desplegado en nube o solución podrá ser excluido del CPSTIC por cualquiera de los siguientes motivos:

- **Alcance de la fecha de vigencia** (dos años o, para los productos *on-premise*, la fecha de fin de soporte de seguridad, lo que ocurra antes) sin que se produzca la renovación o, en su caso, la ampliación.
- **Revocación o caducidad de alguna de las certificaciones requeridas** (*Common Criteria*, LINCE o conformidad con el ENS). Para las certificaciones *Common Criteria* o LINCE se considerará una validez máxima de cinco (5) años.
- **Incumplimiento de los RFS vigentes** en el momento de la revisión de validez.
- **Existencia de vulnerabilidades críticas no corregidas.** Podrá solicitarse al fabricante un informe de impacto; si la vulnerabilidad es explotable siguiendo el PES, la entrada será excluida. En productos de seguridad desplegados en nube, una vulnerabilidad crítica supone un PGC igual a 0 (veredicto FALLA de la evaluación CICLON) y la exclusión.
- **No entrega del Procedimiento de Empleo Seguro (PES)** dentro del periodo de inclusión provisional de seis (6) meses.
- **Finalización del soporte de seguridad** por parte del fabricante, quien estará obligado a notificarlo al CPSTIC.
- **Resultado desfavorable de la revisión periódica** de las evidencias, incluido, para las soluciones de Conformidad y Gobernanza, un resultado desfavorable en la actualización de las pruebas de penetración. En la cualificación para ALTA a partir de una certificación LINCE, si el análisis periódico no cumple los requisitos de categoría ALTA, el producto pasará a categoría MEDIA, y si es desfavorable

también frente a los requisitos de categoría MEDIA, será excluido del CPSTIC (apartado 4.1.1.2).

7. DISTINTIVOS DE INCLUSIÓN

7.1 CONDICIONES DE USO

La inclusión de un producto, producto de seguridad desplegado en nube o solución en el CPSTIC podrá representarse mediante los **distintivos de inclusión** expedidos por el CCN, específicos de cada listado. Su uso queda condicionado a la inclusión en el CPSTIC. El solicitante podrá, de forma voluntaria, dar publicidad a las entradas cualificadas o incluidas exhibiendo el distintivo correspondiente en su documentación técnica o comercial, en cualquier formato. Los distintivos vigentes se encuentran en la sección "MEDIA" de la web del CPSTIC (https://cpstic.ccn.cni.es/es/sobre-el-cpstic/media).

Queda expresamente prohibida la manipulación o reproducción parcial de los distintivos, así como su utilización sin indicar a qué producto o solución están asociados. Excluida una entrada del CPSTIC (apartado 6.3), el solicitante deberá retirar los distintivos empleados en su documentación.

7.2 DISTINTIVO DE PRODUCTO CUALIFICADO

Corresponde a los productos de seguridad *on-premise* cualificados. Presenta el aspecto siguiente, incluyendo la categoría máxima para la que el producto está cualificado (MEDIA o ALTA). La Tabla 7 indica los sistemas para los que resulta adecuado cada distintivo.



Figura 5. Distintivo de Producto Cualificado — Categoría ALTA



Figura 6. Distintivo de Producto Cualificado — Categoría MEDIA

Utilización de productos en el ENS de acuerdo con el distintivo	
Cualificación obtenida	**Adecuado para sistemas**
ALTA	ENS Cat. ALTA · ENS Cat. MEDIA · ENS Cat. BÁSICA
MEDIA	ENS Cat. MEDIA · ENS Cat. BÁSICA

Tabla 7. Utilización de productos en el ENS según el distintivo

7.3 DISTINTIVO DE PRODUCTO DE SEGURIDAD DESPLEGADO EN NUBE CUALIFICADO

Corresponde a los productos de seguridad desplegados en nube cualificados. Presenta el aspecto siguiente, incluyendo la categoría máxima para la que está cualificado (MEDIA o ALTA). La Tabla 8 indica los sistemas para los que resulta adecuado cada distintivo.



Figura 7. Distintivo de Producto de seguridad desplegado en nube Cualificado — Categoría ALTA



Figura 8. Distintivo de Producto de seguridad desplegado en nube Cualificado — Categoría MEDIA

Utilización de productos de seguridad desplegados en nube en el ENS de acuerdo con el distintivo	
Cualificación obtenida	**Adecuado para sistemas**
ALTA	ENS Cat. ALTA · ENS Cat. MEDIA · ENS Cat. BÁSICA
MEDIA	ENS Cat. MEDIA · ENS Cat. BÁSICA

Tabla 8. Utilización de productos de seguridad desplegados en nube en el ENS según el distintivo

7.4 DISTINTIVO DE CONFORMIDAD Y GOBERNANZA

Corresponde a las soluciones incluidas en el listado de Conformidad y Gobernanza. Presenta el aspecto siguiente.



Figura 9. Distintivo de Conformidad y Gobernanza

8. REFERENCIAS

[1] Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional.

[2] Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

[3] CCN-STIC-105 Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC).

[4] CCN-STIC-102 Procedimiento para la Aprobación de Productos de seguridad TIC para manejar información Nacional clasificada.

[5] CCN-STIC-140 Taxonomía de referencia para productos de Seguridad TIC.

[6] CCN-STIC-2003 Plantilla de Declaración de Seguridad (LINCE).

[7] Anexo A CCN-STIC-2010 Plantilla de Declaración de Seguridad (DS).

[8] Anexo B CCN-STIC-2010 Plantilla para el Documento de Arquitectura del Servicio (DAS).

[9] Anexo A CCN-STIC-106 Plantilla de Justificación de Requisitos (JR).

[10] Anexo B CCN-STIC-106 Plantilla de Informe de Análisis Diferencial (IAD).

[11] Anexo C CCN-STIC-106 Plantilla de Procedimiento de Empleo Seguro (PES).

[12] CCN-STIC-2004 Plantilla del Informe Técnico de Evaluación de la Certificación Nacional Esencial de Seguridad (LINCE).

[13] CCN-STIC-2010 Metodología de Evaluación de Productos en la Nube (CICLON).

[14] CCN-STIC-2001 Definición de la Certificación Nacional Esencial de Seguridad (LINCE).

[15] CCN-STIC-2002 Metodología de Evaluación para la Certificación Nacional.

[16] CCN-STIC-807 Criptología de empleo en el ENS.

[17] CCN-STIC 2030 Metodología de evaluación de seguridad en entornos web.

9. ABREVIATURAS

CC	Criterios Comunes / Common Criteria.
CCN	Centro Criptológico Nacional.
CICLON	Metodología de Evaluación de Productos en la Nube (CCN-STIC-2010).
COM-INI	Comunicación de Inicio de Expediente de inclusión.
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación.
DAS	Documento de Arquitectura del Servicio.
DS	Declaración de Seguridad / Security Target.
ENECSTI	Esquema Nacional de Evaluación y Certificación de la Seguridad de las TIC.
ENS	Esquema Nacional de Seguridad.
FOR	Formulario.
GRC	Gobierno, Riesgo y Cumplimiento.
IaaS	Infrastructure as a Service / Infraestructura como servicio.
IAD	Informe de Análisis Diferencial.
ITE	Informe Técnico de Evaluación.
ITI	Informe Técnico de Inclusión.
ITM	Informe Técnico de Monitorización.
JR	Justificación de Requisitos.
LINCE	Certificación Nacional Esencial de Seguridad.
OTAN	Organización del Tratado del Atlántico Norte.
PaaS	Platform as a Service / Plataforma como servicio.
PES	Procedimiento de Empleo Seguro.
PGC	Porcentaje de Garantía Compuesto.
PGE	Porcentaje de Garantía de Evaluación.
PGM	Porcentaje de Garantía de Monitorización.
RFS	Requisitos Fundamentales de Seguridad.
RGPD	Reglamento General de Protección de Datos.
RITI	Resultado del Informe Técnico de Inclusión.
RRPDS	Resultado de la Revisión de la Propuesta de Declaración de Seguridad.
SaaS	Software as a Service / Software como servicio.
STIC	Seguridad de las Tecnologías de la Información y la Comunicación.
TIC	Tecnologías de la Información y la Comunicación.
TOE	Target of Evaluation / Objeto de evaluación.
UE	Unión Europea.