CCN
CENTRO CRIPTOLÓGICO NACIONAL

Procedimiento de Seguridad de las TIC
CCN-STIC 102

Procedimiento para la Aprobación de Productos de Seguridad TIC para manejar Información Clasificada

Octubre 2017

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.02.07 13:16:51 +01'00'

© Centro Criptológico Nacional, 2017
NIPO: 083-19-001-9

Fecha de Edición: octubre 2017

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

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.

PRÓLOGO

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

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

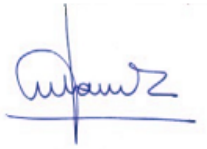
Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad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

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

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

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

Octubre de 2017



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN 5
2. OBJETIVO 6
3. ALCANCE 6
4. DESCRIPCIÓN DEL PROCESO DE APROBACIÓN PARA MANEJAR INFORMACIÓN NACIONAL CLASIFICADA 7
5. PROCESO DE APROBACIÓN PARA MANEJAR INFORMACIÓN CLASIFICADA DE OTROS ORGANISMOS 11
6. BIBLIOGRAFÍA DE REFERENCIA 12
7. ABREVIATURAS 12

ANEXOS

ANEXO A. FORMULARIO SOLICITUD DE APROBACIÓN DE PRODUCTO DE SEGURIDAD TIC 13

1. INTRODUCCIÓN

1. La adquisición de un producto de seguridad TIC cuando va a manejar información nacional clasificada debe estar precedida por la comprobación de la adecuación de los mecanismos implementados en el producto para proteger dicha información.
2. La evaluación y certificación de un producto de seguridad TIC son procesos que permiten valorar y acreditar la capacidad de un producto para manejar información de forma segura. En España, esta responsabilidad está asignada al Centro Criptológica Nacional (CCN) a través del RD 421/2004 de 12 de marzo. En su Artículo 1 se establece que el Director del CCN es la autoridad de certificación de la seguridad de las tecnologías de la información y comunicaciones y autoridad de certificación criptológica. En los artículos 2.1 y 2.2d. se establece que, dentro del ámbito de actuación del CCN está el valorar y acreditar la capacidad de los productos de cifra y de los sistemas de las tecnologías de la información, que incluyan medios de cifra, para procesar, almacenar o transmitir información de forma segura.
3. La evaluación y certificación de un producto de seguridad TIC debe abarcar aspectos relativos a la implementación de los requisitos funcionales de seguridad en dicho producto, así como otros aspectos del producto que aumentan su seguridad y la mantengan a lo largo de la vida útil del mismo.
4. En el caso de que el producto utilice criptografía para proteger la confidencialidad, integridad, autenticidad y/o el no repudio de la información nacional clasificada, también es fundamental abarcar los aspectos relativos a la seguridad criptológica de los algoritmos empleados, así como los relacionados con su implementación en el equipo o sistema donde se incluyan, así como la eficacia de sus mecanismos de autoprotección.
5. En el caso en el que el producto de seguridad TIC supere los mínimos requisitos de seguridad exigibles para proteger información nacional clasificada Confidencial o superior, también será necesario verificar su seguridad frente a emanaciones no deseadas (TEMPEST).
6. El producto de seguridad TIC se aprobará para una versión concreta del producto y con una configuración determinada y de acuerdo a unas normas de utilización que serán descritas en el procedimiento de empleo del producto.
7. El producto aprobado por el CCN deberá distribuirse junto con el procedimiento de empleo.

2. OBJETIVO

8. El objeto del presente documento es detallar el proceso de Aprobación de los **productos de Seguridad TIC**[1] para manejar información nacional clasificada.

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

3. ALCANCE

10. La presente guía es de aplicación para aquellos productos de seguridad TIC que vayan a ser adquiridos para su empleo en sistemas que vayan a procesar información nacional clasificada.

11. En el caso de que el producto de seguridad TIC necesite de otros productos de seguridad asociados para su funcionamiento, como pueden ser centros de gestión, generadores de números aleatorios, dispositivos de transporte de claves, etc., estos elementos deben incluirse en el proceso de aprobación o encontrarse ya aprobados para el mismo nivel de clasificación o superior.

[1] Según la definición del apartado 2807 PRODUCTO DE SEGURIDAD TIC incluida en la Guía CCN-STIC 401 [REF4]

4. DESCRIPCIÓN DEL PROCESO DE APROBACIÓN PARA MANEJAR INFORMACIÓN NACIONAL CLASIFICADA

12. El proceso de Aprobación para manejar información nacional clasificada es el resultado de la evaluación y certificación favorable de los aspectos funcionales y de seguridad de un producto.

13. El proceso comienza con la solicitud al Centro Criptológico Nacional (CCN), a través del Organismo de Certificación[2] (OC), de la Aprobación para manejar información nacional clasificada (ver ANEXO A). Esta solicitud debe estar respaldada formalmente por parte de un organismo de la Administración, que deberá justificar la necesidad del Producto de Seguridad TIC. Junto a la Solicitud de Aprobación se adjuntará la Declaración de Seguridad (DS) según especifica Common Criteria[3] del producto, una descripción detallada de su arquitectura, tanto hardware como software así como una propuesta de guía de instalación, configuración y uso seguro.

14. Una vez revisada la Solicitud de Aprobación, y tras requerir el Organismo de Certificación la **subsanación de cualquier defecto de forma** que pueda presentar la misma, se notificará al solicitante el **inicio del proceso de Aprobación**.

15. Se establece un plazo máximo de **un mes** para responder a los requerimientos del CCN. Transcurrido este plazo, si no se han subsanado los defectos de forma encontrados, se procederá al cierre del proceso de Aprobación.

16. El personal asignado por el CCN al proceso de Aprobación revisará la documentación presentada por el solicitante y elaborará un ***"Informe de Conformidad de Requisitos Fundamentales de Seguridad"***. Para elaborar dicho informe de conformidad, se tomarán como referencia las guías **CCN-STIC 130 Requisitos de Aprobación de Productos de Cifra para Manejar Información Nacional Clasificada** [REF2] y **CCN-STIC 140 Taxonomías de Referencia para Productos de Seguridad TIC** [REF6]

17. Se realizará una reunión en la que participará el personal del solicitante y del CCN involucrados en el proceso de Aprobación. En esa reunión se comunicará al solicitante el ***"Informe de Conformidad de Requisitos Fundamentales de Seguridad"*** así como las **certificaciones y evaluaciones complementarias que necesitará el producto para obtener la Aprobación** para manejar información nacional clasificada.

[2] Organismo de Certificación del Centro Criptológico Nacional ver https://oc.ccn.cni.es
[3] También denominado Security Target (ST), www.commoncriteriaportal.org/cc Part1: Introduction and general model, Sección A.

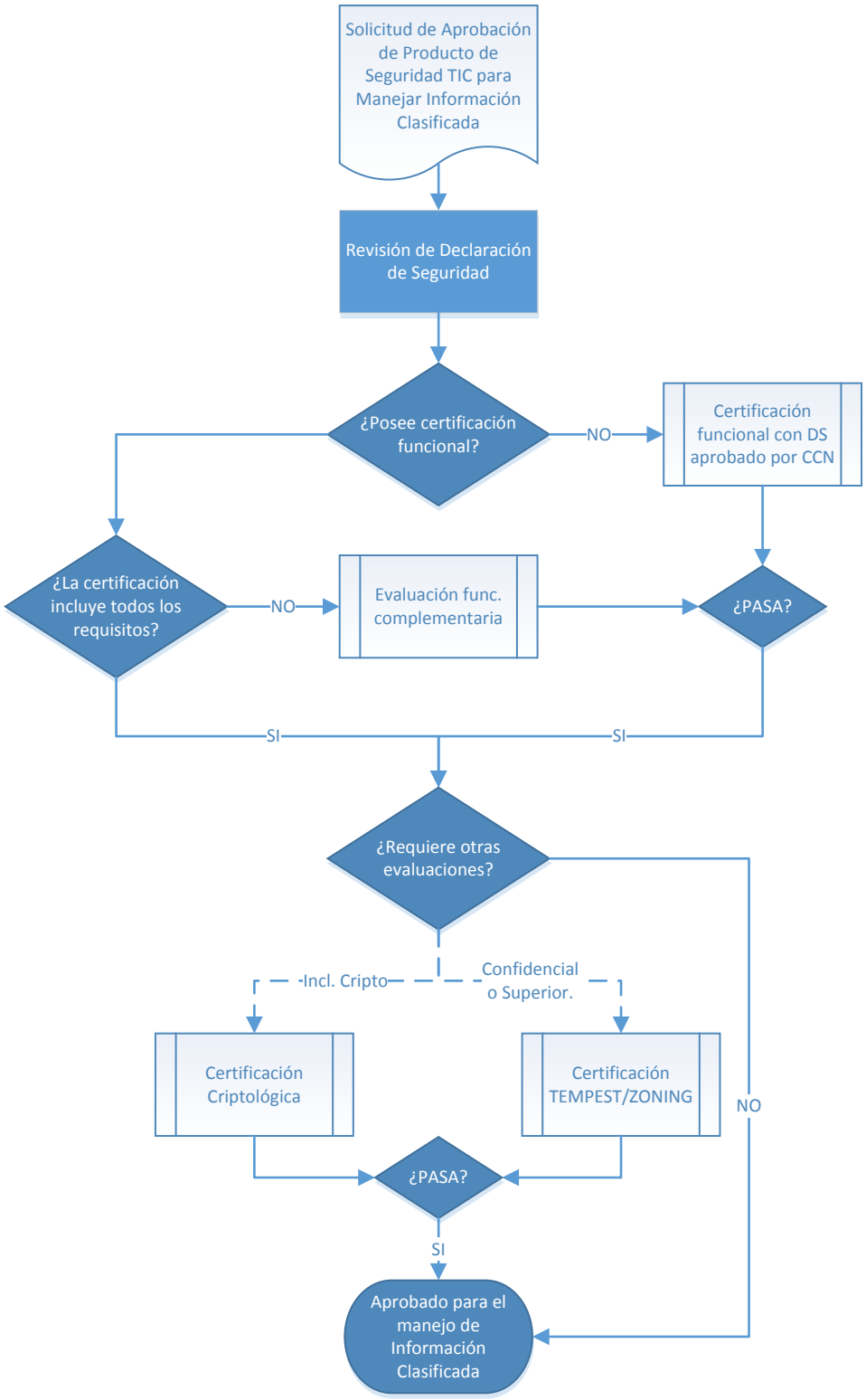


Figura 1. Procedimiento de Aprobación de Productos STIC

18. Una vez determinadas las certificaciones y evaluaciones requeridas, el solicitante iniciará el proceso de Certificación Funcional (si no la tuviera previamente), Criptológica y Tempest según sea requerido.

CLASIFICACIÓN	REQUISITOS			
	FUNCIONAL	EVALUACIÓN COMPLEMENTARIA	CRIPTO	TEMPEST
CONFIDENCIAL O SUPERIOR	Validación Declaración de Seguridad (DS)	Evaluación complementaria en laboratorios del ENECSTI[4]	Certificación Cripto. CCN (profundidad de la evaluación depende del nivel de clasificación)	Certificación TEMPEST CCN
DIFUSIÓN LIMITADA	Validación DS Puede estar certificado por OC extranjero			--

Figura 2. Requisitos para la Aprobación

19. En el caso de que el producto de seguridad TIC requiera otras certificaciones además de la funcional, y dada la complejidad que supone realizar modificaciones al producto tras la misma, en paralelo con este proceso el solicitante entregará al CCN la documentación técnica inicial que corresponda, según las guías **CCN-STIC 130** [REF2] y **CCN-STIC 151 Evaluación y Clasificación TEMPEST de Equipos** [REF3]. Esto permitirá al CCN detectar posibles vulnerabilidades o funciones de seguridad que a priori no cumplan con la fortaleza necesaria para proteger información nacional clasificada y poder así solicitar las modificaciones necesarias al producto.

20. Una vez obtenida la Certificación Funcional del producto, se iniciarán las certificaciones adicionales que fueran requeridas. Para ello, se realizará una reunión entre el personal del solicitante y del CCN, en la que el solicitante entregará al CCN toda la documentación técnica y el material que sea necesario para llevar a cabo las evaluaciones adicionales que corresponda según se indica en las guías CCN-STIC 130 [REF2] y CCN-STIC 151 [REF3].

21. En **casos excepcionales**, si el organismo de la Administración que avala el proceso de Aprobación necesita de forma urgente el producto, podrá solicitar una aprobación con carácter interino que se otorgará una vez se hayan verificado parámetros básicos de seguridad funcional, criptológica y de emanaciones y siempre que se haya iniciado la evaluación funcional del producto. Dicha autorización interina, tendrá carácter temporal hasta que se hayan finalizado todas las certificaciones requeridas. El uso del producto de seguridad TIC estará restringido al ámbito para el que se haya autorizado expresamente.

22. Una vez obtenidas las certificaciones requeridas y una vez estudiados y revisados todos los informes técnicos de evaluación y pruebas del producto se expedirá la **"Aprobación de Producto de Seguridad TIC para manejar Información Nacional Clasificada"**, donde figurará el **máximo nivel de clasificación que está autorizado a manejar** y el **plazo de vigencia de la misma**.

[4] Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información ver sección laboratorios acreditados en https://oc.ccn.cni.es

23. La correspondiente "Aprobación de Producto de Seguridad TIC para manejar Información Nacional Clasificada" será firmada por el Secretario de Estado Director del Centro Nacional de Inteligencia que, como Director del Centro Criptológico Nacional, es la autoridad de certificación de la seguridad de las tecnologías de la información y autoridad de certificación criptológica (RD 421/2004 de 12 de marzo, Art.1).

24. Una vez finalizado el proceso de Aprobación se enviará al solicitante una copia de la "Aprobación de Producto de Seguridad TIC para manejar Información Nacional Clasificada". Junto con dicha Aprobación se enviará el **Procedimiento de Empleo** del producto, **que debe distribuirse junto con el producto**.

25. Dicho producto **se incluirá en el apartado de productos aprobados del "Catálogo de Productos de Seguridad TIC"** (CCN-STIC 105) [REF1].

26. Si el producto ha superado una evaluación criptológica, se incluirá además en el **"Catálogo de Productos con Certificación Criptológica"** (CCN-STIC 103) [REF5].

27. El proceso de Aprobación debe realizarse sin solución de continuidad, respondiendo el solicitante a los requerimientos que se le realicen en el plazo más breve posible. En todo caso, el proceso deberá completarse en un plazo máximo de **veinticuatro meses desde su inicio** (ver párrafo 14). Transcurrido este plazo, si no se han superado exitosamente las distintas evaluaciones y certificaciones exigidas (ver párrafo 17), se procederá al cierre del proceso de Aprobación.

28. El fabricante deberá **fijar un periodo mínimo de mantenimiento del producto (que deberá ser aceptado por el CCN)** durante el cual se compromete a mantenerlo actualizado resolviendo todas las vulnerabilidades de seguridad que puedan surgir durante dicho periodo.

29. **Para cada nueva versión del producto**, el fabricante se compromete a **entregar al OC un informe de cambios e impacto en la seguridad**. Una vez verificado que los cambios realizados garantizan las características de seguridad del producto, se expedirá una adenda al documento de Aprobación para dicha versión, momento en el cual podrá ser distribuida a los usuarios. En caso contrario, podría ser necesaria una reevaluación parcial, total o incluso implicar la revocación de la Aprobación del producto.

30. El CCN publicará las versiones aprobadas de cada producto. Esto no exime al fabricante de comunicar a sus clientes la existencia de esas nuevas versiones aprobadas por el CCN.

31. **Periódicamente se realiza una reevaluación de los productos aprobados** con el fin de garantizar que sus características de seguridad se mantienen frente a los avances tecnológicos. Dicha reevaluación podría conllevar la reducción del máximo nivel de clasificación que está autorizado a manejar o incluso la revocación de la aprobación si dejara de cumplir los mínimos requisitos de seguridad necesarios para procesar información nacional clasificada.

32. En caso de aparecer vulnerabilidades que afecten a la seguridad del producto durante el periodo de vigencia de la Aprobación, si no se acometen medidas que

las mitiguen o eliminen (manteniendo la funcionalidad del producto) en un plazo razonable y aceptado por el CCN, se procederá a la revocación de dicha Aprobación o a bajar el nivel de clasificación concedido.

33. Una vez finalizado el periodo de vigencia de la Aprobación, se realizará una revisión de dicho producto que podrá conllevar bien el fin definitivo de dicha aprobación, bien una revisión del nivel máximo de clasificación de la información que puede procesar o una prórroga de la misma.

34. Cuando se produzca el fin de la vigencia de una aprobación o la revocación de la misma, el producto será eliminado tanto del **"Catálogo de Productos de Seguridad TIC"** [REF1] **como del "Catálogo de Productos con Certificación Criptológica"** [REF5].

5. PROCESO DE APROBACIÓN PARA MANEJAR INFORMACIÓN CLASIFICADA DE OTROS ORGANISMOS

35. Una vez aprobado el producto nacionalmente si se aspira a obtener aprobaciones adicionales por Organismos Internacionales como la Organización del Tratado del Atlántico Norte (OTAN), la Unión Europea (UE), la Agencia Espacial Europea (*European Space Agency* ESA), hay que tener en cuenta los requisitos específicos de dichos Organismos.

36. En el caso de OTAN, y para productos criptográficos, los requisitos a seguir son los especificados en el documento *"Infosec Technical and Implementation Directive on Cryptographic Security and Cryptographic Mechanisms"* con referencia AC/322-D/0047[REF7].

37. En el caso de UE, y para productos criptográficos, los requisitos a seguir son los especificados en el documento *"IA Security Policy on Cryptography"* con referencia IASP 2 [REF8], así como la normativa aplicable sobre Seguridad de la Información para productos criptográficos que se puede obtener en la web del Consejo de la Unión Europea[5].

[5] http://www.consilium.europa.eu/en/general-secretariat/corporate-policies/classified-information/information-assurance/

6. BIBLIOGRAFÍA DE REFERENCIA[6]

REF1 CCN-STIC 105 Catálogo de Productos de Seguridad TIC (CPSTIC).

REF2 CCN-STIC 130 Requisitos de Aprobación de Productos de Cifra para Manejar Información Nacional Clasificada.

REF3 CCN-STIC 151 Evaluación y Clasificación TEMPEST de Equipos.

REF4 CCN-STIC 401 Glosarios y Abreviaturas.

REF5 CCN-STIC 103 Catálogo de Productos con Certificación Criptológica.

REF6 CCN-STIC 140 Taxonomías de Referencia para Productos de Seguridad TIC.

REF7 AC/322-D/0047 Infosec Technical and Implementation Directive on Cryptographic Security and Cryptographic Mechanisms (OTAN)

REF8 IASP 2 - IA Security Policy on Cryptography (UE)

7. ABREVIATURAS

CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación
DS/ST	Declaración de Seguridad / Security Target
ENECSTI	Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información
ITE	Informe Técnico de Evaluación / Evaluation Technical Report
OC	Organismo de Certificación
PP	Perfil de protección
RD	Real Decreto
STIC	Seguridad de las Tecnologías de la Información y la Comunicación
TIC	Tecnologías de la Información y la Comunicación

[6] Última versión en vigor.

ANEXO A. FORMULARIO SOLICITUD DE APROBACIÓN DE PRODUCTO DE SEGURIDAD TIC

38. La última versión del formulario de solicitud de Aprobación de un Producto de Seguridad TIC para el manejo de información nacional clasificada está disponible en la página web del Organismo de Certificación (https://oc.ccn.cni.es) para su descarga.

39. El formulario consta de los siguientes apartados:

    a) Información del solicitante.

    b) Organismo proponente (aval formal).

    c) Información del producto

    d) Adjuntos:

        - Declaración de seguridad funcional.
        - Descripción detallada de la arquitectura hardware y software, así como un listado de los algoritmos de cifra que utilice (en caso de hacerlo).
        - Guía de instalación, configuración y uso seguro.

    e) Declaración de aceptar y conocer los requisitos de Aprobación de Productos de Seguridad TIC para el manejo de información nacional clasificada.

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