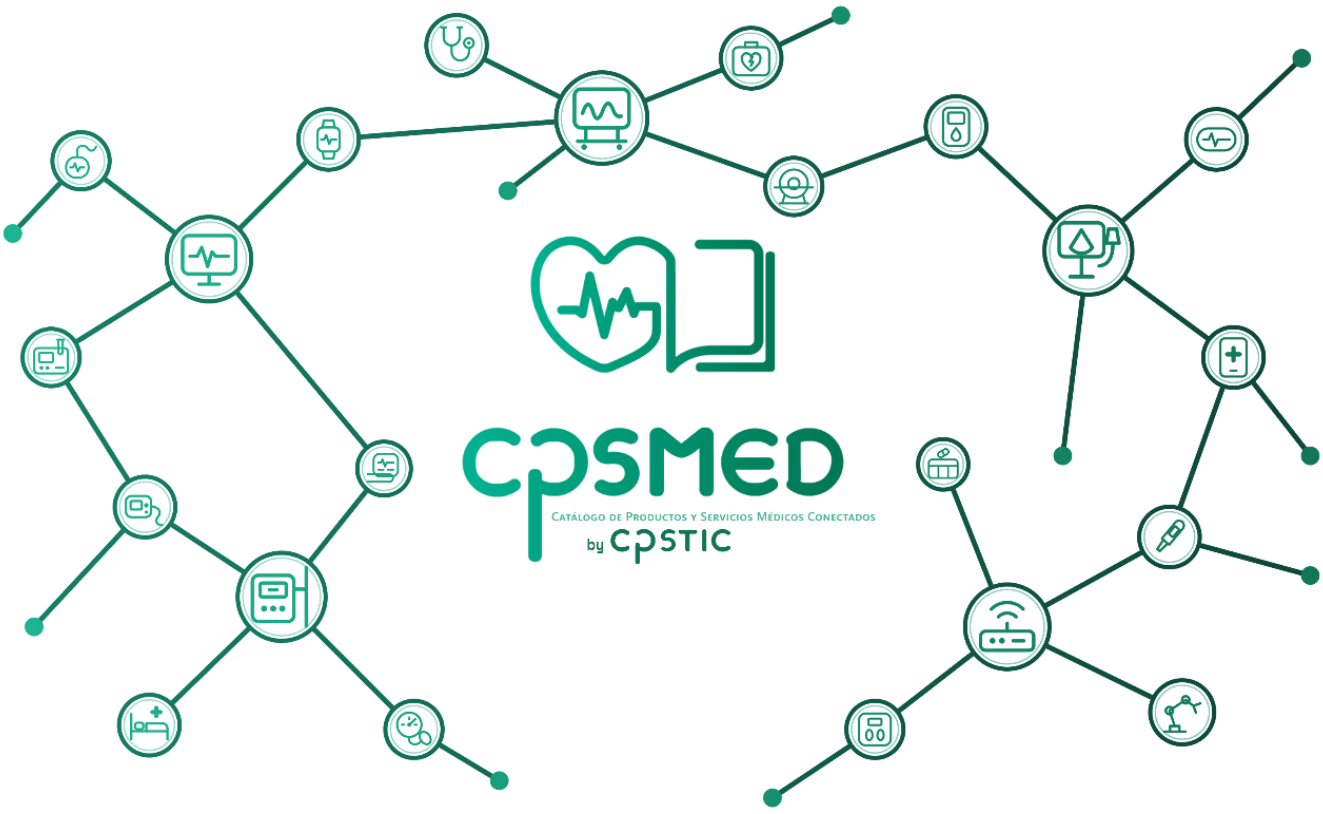
Guía de Seguridad de las TIC
CCN-STIC 163

Plantilla de Informe de Análisis Diferencial (IAD)



Noviembre 2026

Edita:

centro criptológico nacional

centro criptológico nacional

CCN
c=ES, l=MADRID, o=CCN, ou=SELLO ELECTRONICO, 2.5.4.97=VATES-S2800155J, serialNumber=S2800155J, cn=CCN
2026.11.18 08:24:00 +01:00

Versión: 1.0
Fecha de Edición: Noviembre 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.

Esta publicación se distribuye bajo licencia CC BY-NC-ND 4.0 que permite compartir el material en cualquier medio o formato con la condición de reconocer adecuadamente la procedencia «Edita: Ministerio de Defensa. Secretaría General Técnica.» No se puede modificar. No se puede utilizar con fines comerciales.

ÍNDICE

1 INTRODUCCIÓN 5
1.1 OBJETO DEL DOCUMENTO 5
1.2 TIPO DE AMPLIACIÓN 5
1.3 ALCANCE DEL ANÁLISIS 6
1.4 TÉRMINOS EMPLEADOS 6
1.5 INFORMACIÓN DEL SOLICITANTE Y DEL PRODUCTO 7
2 CARACTERIZACIÓN DE LA CERTIFICACIÓN DE PARTIDA 8
2.1 ALCANCE SOLICITADO FRENTE AL ALCANCE DE PARTIDA 8
2.2 ASIGNACIONES Y SELECCIONES RELEVANTES 9
2.3 AMPLIACIONES ANTERIORES 9
3 CRITERIOS DE ANÁLISIS 10
4 IDENTIFICACIÓN DE DIFERENCIAS 11
4.1 MATRIZ DE CARACTERÍSTICAS 11
4.2 AGRUPACIONES TECNOLÓGICAS HOMOGÉNEAS 14
4.3 RELACIÓN DE CAMBIOS ENTRE VERSIONES 14
4.4 RESUMEN DE DIFERENCIAS 15
4.5 IMPACTO REGULATORIO 15
5 REQUISITOS AFECTADOS Y ALCANCE PENDIENTE DE VERIFICACIÓN 17
5.1 RELACIÓN DE REQUISITOS AFECTADOS 17
5.2 EJEMPLOS 17
5.3 MATRIZ DE ALCANCE 19
6 CONFORMIDAD CRIPTOGRÁFICA 20
7 GUÍAS DE INSTALACIÓN Y OPERACIÓN 21
7.1 GUÍAS DEL FABRICANTE 21
7.2 GUÍA CCN-STIC DE LA SERIE 4000 21
8 CONCLUSIONES 22
8.1 CONCLUSIÓN DEL ANÁLISIS 22
8.2 ENTREGABLES 22
9 OBSERVACIONES DEL SOLICITANTE 23
10 DECLARACIÓN RESPONSABLE 24
10.1 DOCUMENTACIÓN APORTADA COMO EVIDENCIA 24

11 REFERENCIAS 26

INSTRUCCIONES DE CUMPLIMENTACIÓN Y ENVÍO

Esta plantilla constituye el Anexo B de la CCN-STIC-163. El documento resultante de su cumplimentación es el Informe de Análisis Diferencial (IAD) del producto y, firmado electrónicamente por el responsable técnico del solicitante, tiene la consideración de declaración responsable.

El IAD se remite junto con la solicitud de inclusión o de ampliación (FOR-CPSMED-02), acompañado de las evidencias relacionadas en la declaración responsable.

Instrucciones de contenido

Los textos en gris y cursiva son instrucciones de cumplimentación y deberán eliminarse del documento final. El texto en negro forma parte del informe y de la declaración responsable que firma el solicitante.

Todos los apartados son de cumplimentación obligatoria. Cuando un apartado no resulte de aplicación, se mantendrá el epígrafe y se hará constar expresamente su no aplicabilidad.

Toda afirmación relativa a la ausencia de impacto deberá justificarse técnicamente y referenciarse a la evidencia que la sustenta.

Las evidencias se aportarán junto a la declaración responsable o, cuando sean públicas, se identificarán indicando la dirección desde la que resultan accesibles.

No se incluirán credenciales, claves, datos de clientes ni contenido de carácter comercial.

Comprobaciones antes del envío

a) *Se han eliminado todos los textos en gris y cursiva, incluidos los ejemplos.*

b) *Los apartados que no resultan de aplicación se mantienen con su justificación.*

c) *Todas las evidencias citadas figuran en la declaración responsable, indicando su forma de aportación.*

d) *El documento está firmado electrónicamente por el responsable técnico del solicitante.*

1 INTRODUCCIÓN

1.1 OBJETO DEL DOCUMENTO

[Este documento es una plantilla de referencia para redactar el Informe de Análisis Diferencial (IAD) contemplado en la guía CCN-STIC-163 [REF1].]

El IAD es una declaración del solicitante, firmada por su responsable técnico, mediante la cual se analiza en qué medida los Requisitos Fundamentales de Seguridad (RFS) de la familia correspondiente de la taxonomía CCN-STIC-142 [REF2] se ven afectados por las diferencias existentes entre el alcance solicitado y el objeto de la certificación aportada, y qué parte de ellos, en su caso, constituye alcance pendiente de verificación. Su aportación no sustituye ni condiciona el pronunciamiento del CCN, que podrá apartarse motivadamente del análisis contenido en él.

El IAD identifica los Requisitos Fundamentales de Seguridad que deben volver a verificarse mediante una Evaluación STIC Complementaria, que podrán ser ninguno cuando las diferencias no impacten en ellos. Cuando el resultado de dicha evaluación es favorable, el expediente continúa con la elaboración del Informe Técnico de Inclusión (ITI) y la comunicación del Resultado del Informe Técnico de Inclusión (RITI).

1.2 TIPO DE AMPLIACIÓN

[El IAD se aporta cuando el alcance que se pretende incluir no coincide con el de la base del análisis, ya sea por incorporar modelos no incluidos en ella o una versión posterior.]

El presente documento, en su totalidad, tiene la consideración de declaración responsable del solicitante y se aporta en todo caso, impacten o no los cambios en los RFS, por lo que su contenido deberá ser completo y veraz. Cuando del análisis se concluya que los cambios introducidos no impactan en los RFS, esta declaración constituye la evidencia sobre la que se sustenta la inclusión del alcance solicitado, sin que resulte necesaria la realización de una Evaluación STIC Complementaria. Por este motivo, la cumplimentación del documento es exhaustiva.

[Indicar el tipo de ampliación al que se refiere el análisis.]

Tipo de ampliación	Aplicable (Sí / No)	Alcance
Ampliación de hardware — modelos		[Relación de modelos adicionales]
Ampliación de software — versión		[Versión candidata y versión de partida]

1.3 ALCANCE DEL ANÁLISIS

El análisis contenido en este documento se refiere exclusivamente a los RFS de la familia o familias de la CCN-STIC-142 para las que se solicita la inclusión en el CPSMED. Queda fuera de su alcance cualquier otra funcionalidad de seguridad del producto.

Queda asimismo fuera del alcance de esta plantilla el análisis de la cobertura de los RFS por la declaración de seguridad, que se realiza mediante la plantilla de Justificación de Requisitos (JR) recogida en el Anexo A de la CCN-STIC-163 [REF3] cuando dicha guía lo exija.

El análisis del impacto regulatorio de los cambios conforme a la normativa de productos sanitarios se recoge, a efectos informativos, en el apartado 4.5, sin que sustituya a la evaluación de la conformidad que corresponda al fabricante o al organismo notificado.

1.4 TÉRMINOS EMPLEADOS

A los efectos de este documento se emplean los términos siguientes:

a) Alcance de partida: conjunto de modelos y versiones del producto amparados por la certificación de partida o por el último IAD aceptado por el CCN, que constituye la referencia del análisis.

b) Alcance solicitado: conjunto de modelos y versiones del producto cuya inclusión se solicita.

c) Agrupación tecnológica homogénea: conjunto de modelos que comparten plataforma, firmware y componentes relevantes para la seguridad, y que se tratan como una unidad en el análisis.

d) DIF-HW-XX y DIF-SW-XX: códigos con los que se identifican, de forma unívoca, las diferencias de plataforma y los cambios entre versiones, respectivamente.

e) Alcance pendiente de verificación: parte del alcance solicitado que, por verse afectada por las diferencias identificadas, debe verificarse antes de ampliar la inclusión.

f) Evaluación STIC Complementaria: evaluación, realizada por un laboratorio acreditado en el ENECSTI, que verifica los requisitos afectados cuando las diferencias impactan en ellos.

g) Requisitos Fundamentales de Seguridad (RFS): requisitos exigibles a la familia o familias solicitadas, definidos en los anexos de la taxonomía CCN-STIC-142 [REF2] o, para las familias cuyo anexo no se haya publicado, comunicados por escrito por el CCN conforme al apartado 3.2 de la CCN-STIC-163.

h) Cambio significativo: modificación del producto sanitario que, conforme al MDR o al IVDR, requiere la evaluación o la aprobación del organismo notificado, o una nueva declaración UE de conformidad, antes de su comercialización.

1.5 INFORMACIÓN DEL SOLICITANTE Y DEL PRODUCTO

Nombre del solicitante	
Fabricante o desarrollador	
Responsable técnico (nombre, cargo y datos de contacto)	
Nombre comercial del producto	
Familia(s) de la taxonomía (CCN-STIC-142) y anexo de RFS	
Finalidad prevista	
Número de expediente CPSMED	
Situación actual en el CPSMED (no incluido / incluido / inclusión provisional)	
Fecha del documento	

2 CARACTERIZACIÓN DE LA CERTIFICACIÓN DE PARTIDA

El presente apartado recoge qué ha sido efectivamente evaluado y cuál es la base del presente análisis: la certificación de partida o, cuando el producto haya sido objeto de ampliaciones anteriores, el último IAD aceptado por el CCN. El alcance recogido en esa base se denomina alcance de partida y constituye la referencia frente a la que se realiza el análisis de los apartados siguientes.

Esquema de certificación (LINCE / Common Criteria / UL 2900-2-1 / específica de la familia, p. ej. IEEE 2621)	
Referencia y fecha del certificado	
Organismo de certificación y laboratorio	
Referencia, versión y fecha de la declaración de seguridad o del informe de certificación	
Pruebas exigidas por el CCN sobre los componentes de inteligencia artificial o desplegados en la nube, si las hubo (referencia y fecha)	
Modelos y versiones de partida	
Base del presente análisis	[Certificación de partida o IAD anterior, indicando su referencia y fecha]

2.1 ALCANCE SOLICITADO FRENTE AL ALCANCE DE PARTIDA

[Permite identificar en qué dimensiones difiere el alcance solicitado del de partida.]

Dimensión	Alcance de partida	Alcance solicitado
Modelos		
Versión de firmware o software		

Dimensión	Alcance de partida	Alcance solicitado
Configuración		

2.2 ASIGNACIONES Y SELECCIONES RELEVANTES

[Relacionar las asignaciones y selecciones de la declaración de seguridad o del alcance de la certificación que condicionan la cobertura de los RFS, en particular las relativas a mecanismos criptográficos, protocolos, métodos de autenticación y mecanismos de actualización.]

SFR o requisito de la norma	Asignación o selección declarada	RFS de la taxonomía afectado

2.3 AMPLIACIONES ANTERIORES

Cuando el producto haya sido objeto de ampliaciones anteriores, se relacionarán los IAD presentados con anterioridad y se indicará en el apartado 2 cuál de ellos, o la certificación, constituye la base del presente análisis.

IAD anterior (referencia y fecha)	Alcance incorporado (modelos o versión)	Expediente o resolución del CCN

3 CRITERIOS DE ANÁLISIS

El análisis parte de las diferencias identificadas en el apartado 4 y determina, para cada una de ellas, los RFS cuya implementación se ve afectada. Los requisitos afectados constituyen el alcance pendiente de verificación; el resto de los RFS de la familia no requieren verificación adicional.

Las declaraciones de ausencia de impacto contenidas en este documento se justifican técnicamente. En particular, no se considera suficiente la mera identidad del firmware cuando las diferencias afecten a componentes que participen en la implementación de mecanismos criptográficos, en el almacenamiento de claves o credenciales, en las fuentes de entropía, en el arranque seguro o en la verificación de integridad.

En los productos sanitarios conectados tampoco se considerará suficiente cuando las diferencias afecten a los componentes que intervienen en las interfaces inalámbricas y en el emparejamiento con otros dispositivos, en el subsistema de alarmas clínicas, en la administración de la terapia o en el funcionamiento autónomo ante la pérdida de conectividad.

Los requisitos asociados a funcionalidad de seguridad introducida por la versión candidata se consideran siempre afectados, haciéndose constar en la justificación que su origen es la propia ampliación y no un defecto de la certificación de partida.

De lo anterior se desprende que los modelos adicionales respecto de los cuales se declare y justifique la ausencia de impacto no generan alcance pendiente de verificación y no requieren pruebas individualizadas.

4 IDENTIFICACIÓN DE DIFERENCIAS

El presente apartado recoge la identificación exhaustiva de las diferencias existentes respecto al alcance de partida, que constituyen la entrada del análisis del apartado 5. Cada diferencia se identifica de forma unívoca mediante el código DIF-HW-XX, para las diferencias de plataforma recogidas en el apartado 4.1, y DIF-SW-XX, para los cambios entre versiones recogidos en el apartado 4.3.

4.1 MATRIZ DE CARACTERÍSTICAS

[Cumplimentar una columna por cada modelo adicional o agrupación tecnológica homogénea. Añadir cuantas filas resulten necesarias. Las filas relacionadas tienen carácter orientativo: se mantendrán únicamente las que resulten aplicables a las características del producto y se añadirán las que sean propias de este. En la columna "Diferencia" se indicará si existe divergencia respecto al TOE certificado y, en caso afirmativo, el identificador DIF-HW-XX.]

Característica	Alcance de partida	Modelo o agrupación 1	Modelo o agrupación n	Diferencia
Referencia comercial				
Chasis y factor de forma				
Procesador (CPU / SoC): fabricante, familia y modelo				
Memoria y almacenamiento no volátil				
Módulo o acelerador criptográfico				
Fuente de entropía o generador de números aleatorios				

Característica	Alcance de partida	Modelo o agrupación 1	Modelo o agrupación n	Diferencia
Almacenamiento seguro de claves (TPM, HSM, secure element)				
Arranque seguro y verificación de integridad				
Interfaces de red				
Interfaces de gestión				
Otros componentes relevantes para la seguridad				
Firmware o software: denominación y versión				
Imagen de firmware o software: identificador y hash				
Librerías criptográficas y componentes de terceros				
Funcionalidades de seguridad soportadas				
Capacidad y rendimiento				

Característica	Alcance de partida	Modelo o agrupación 1	Modelo o agrupación n	Diferencia
Interfaces inalámbricas (BLE, NFC, Wi-Fi, radiofrecuencia propietaria)				
Mecanismo de emparejamiento y asociación con otros dispositivos				
Subsistema de alarmas clínicas				
Componentes de administración de la terapia o de adquisición de datos clínicos				
Aplicación móvil asociada y plataformas móviles compatibles (versión de sistema operativo)				
Biblioteca de fármacos, algoritmo de control o parámetros terapéuticos				
Componentes de inteligencia artificial (modelo, versión y función)				

Característica	Alcance de partida	Modelo o agrupación 1	Modelo o agrupación n	Diferencia
Componentes desplegados en la nube (servicio, versión y función)				
Lista de componentes software (SBOM)				

4.2 AGRUPACIONES TECNOLÓGICAS HOMOGÉNEAS

Los modelos que comparten plataforma, firmware y componentes relevantes para la seguridad se agrupan a efectos del análisis, justificando la homogeneidad del grupo. Las agrupaciones así definidas se emplean como unidad de referencia en la matriz de alcance del apartado 5.

Agrupación	Modelos incluidos	Justificación de la homogeneidad
AGR-01		
AGR-n		

4.3 RELACIÓN DE CAMBIOS ENTRE VERSIONES

Cuando la ampliación se refiere a una versión posterior, se relaciona la totalidad de los cambios existentes entre la versión de partida y la versión candidata, incluidas las versiones intermedias.

[Se aporta como evidencia obligatoria el documento de changelog o de detalle de cambios del producto, con el nivel de granularidad suficiente para identificar los componentes afectados por cada cambio. Este documento se relaciona en el apartado 11.]

Id.	Versión	Tipo de cambio	Descripción	Componente afectado

Id.	Versión	Tipo de cambio	Descripción	Componente afectado
DIF-SW-01		[Corrección de errores / Mejora funcional / Nueva funcionalidad de seguridad / Actualización de componente de terceros / Corrección de vulnerabilidad]		
DIF-SW-n				

4.4 RESUMEN DE DIFERENCIAS

Id.	Descripción resumida	Modelos, agrupaciones o versiones afectados	RFS potencialmente afectados
DIF-HW-01			
DIF-SW-n			

[Cuando no se ha identificado ninguna diferencia en alguna de las categorías anteriores, se hace constar expresamente.]

4.5 IMPACTO REGULATORIO

[Indicar si los cambios analizados constituyen un cambio significativo del producto sanitario conforme al MDR o al IVDR y, en su caso, el estado de su evaluación por el organismo notificado. Esta información se aporta a efectos informativos y no sustituye a la evaluación de la conformidad.]

¿Constituyen los cambios un cambio significativo conforme al MDR / IVDR?: [Sí / No]

¿Se modifica la declaración UE de conformidad o el certificado del organismo notificado?: [Sí / No; indicar referencia]

¿Afectan los cambios a los componentes de inteligencia artificial o desplegados en la nube del producto?: [Sí / No; en caso afirmativo, describir los cambios; el CCN podrá exigir sobre dichos componentes las pruebas que considere oportunas]

Justificación: [Motivar la respuesta]

5 REQUISITOS AFECTADOS Y ALCANCE PENDIENTE DE VERIFICACIÓN

Se relacionan los RFS de la familia [indicar familia], conforme a la nomenclatura del anexo correspondiente de la CCN-STIC-142 [REF2], cuya implementación se ve afectada por las diferencias identificadas en el apartado 4. Los RFS no relacionados no se ven afectados por dichas diferencias y no generan alcance pendiente de verificación.

5.1 RELACIÓN DE REQUISITOS AFECTADOS

[Incluir una fila por cada RFS afectado. El enunciado del alcance pendiente debe ser autocontenido y verificable, de modo que pueda trasladarse directamente al plan de evaluación.]

RFS	Diferencias asociadas	Justificación del impacto	Modelos, agrupaciones o versiones afectados	Alcance pendiente de verificación
[ID]	[DIF-HW-XX / DIF-SW-XX]	[Justificación técnica]	[Modelos, agrupaciones o versiones]	[Enunciado de lo pendiente de verificación]

5.2 EJEMPLOS

[Los ejemplos siguientes se incluyen a efectos ilustrativos y deberán eliminarse del documento final.]

RFS	Diferencias asociadas	Justificación del impacto	Modelos, agrupaciones o versiones afectados	Alcance pendiente de verificación

RFS	Diferencias asociadas	Justificación del impacto	Modelos, agrupaciones o versiones afectados	Alcance pendiente de verificación
CIF.1	*DIF-HW-04*	*La agrupación AGR-02 incorpora un módulo de comunicaciones BLE de distinto fabricante que realiza el cifrado del enlace en hardware. Aunque la biblioteca criptográfica y la configuración de algoritmos permanecen inalteradas, el cifrado del canal inalámbrico se delega en un componente distinto del evaluado.*	*AGR-02*	*Verificar que los mecanismos criptográficos empleados por la agrupación AGR-02 en el enlace inalámbrico coinciden con los declarados y se encuentran entre los autorizados por el CCN (CCN-STIC-807).*

RFS	Diferencias asociadas	Justificación del impacto	Modelos, agrupaciones o versiones afectados	Alcance pendiente de verificación
ASO.2	*DIF-SW-07*	*La versión candidata sustituye la biblioteca que implementa el emparejamiento con el mando remoto y la generación del código de emparejamiento, funcionalidad directamente asociada al requisito.*	*Versión candidata*	*Verificar en la versión candidata el mecanismo de confirmación de la asociación, incluidas la generación aleatoria y la longitud del código de emparejamiento, así como la ventana temporal de asociación (ASO.3).*

5.3 MATRIZ DE ALCANCE

[Cumplimentar cuando existan requisitos cuyo alcance pendiente no abarque la totalidad del alcance solicitado. Podrán emplearse como columnas los modelos, las agrupaciones tecnológicas o las versiones que resulten pertinentes.]

Requisito	Alcance de partida	AGR-01 / Modelo 1	AGR-n / Modelo n	Versión candidata
[ID]				

6 CONFORMIDAD CRIPTOGRÁFICA

La conformidad de los mecanismos criptográficos con la guía CCN-STIC-807 [REF7] se analiza en este apartado de forma transversal, dado que un mismo mecanismo puede incidir sobre varios requisitos y que su valoración depende de las asignaciones y selecciones concretas declaradas, y no de la mera presencia del SFR correspondiente.

Se relacionan los mecanismos criptográficos empleados por el producto que se ven afectados por las diferencias identificadas en el apartado 4, indicando su clasificación conforme a [REF7].

Mecanismo, longitud y modo	Uso en el producto	Clasificación según [REF7]	RFS afectados	Conforme (Sí / No)
	[Cifrado de datos / Establecimiento de claves / Firma / Resumen / Autenticación de mensajes / Derivación de claves]	[Recomendado / Legado / No incluido]		

[Cuando un mecanismo no se encuentra clasificado como recomendado, o cuando la declaración de seguridad no permite determinar cuál es el mecanismo efectivamente empleado, se hace constar y se refleja en el requisito correspondiente del apartado 5, así como en el alcance pendiente de verificación].

[Deberá prestarse especial atención a las funciones pseudoaleatorias, a los grupos Diffie-Hellman y a los esquemas de establecimiento de clave, por ser habituales los casos en que la declaración de seguridad no los concreta o incluye opciones no recomendadas.]

7 GUÍAS DE INSTALACIÓN Y OPERACIÓN

El presente apartado analiza la vigencia de la documentación de instalación y operación respecto al alcance solicitado, dado que la configuración segura del producto forma parte de las condiciones de su inclusión.

7.1 GUÍAS DEL FABRICANTE

Guía (denominación, versión y fecha)	Incluida en el alcance de partida (Sí / No)	¿Contempla el alcance solicitado?	Actuación prevista
			[Ninguna / Actualización de la guía]

7.2 GUÍA CCN-STIC DE LA SERIE 4000

[Se declara expresamente si la inclusión del alcance solicitado exige o no la modificación de la guía CCN-STIC de la serie 4000 publicada para el producto, identificándola por su denominación concreta.]

Guía CCN-STIC de la serie 4000 publicada para el producto: *[Indicar la denominación concreta y la versión, o hacer constar que no existe guía publicada]*

¿Procede su modificación?: *[Sí / No]*

Justificación: *[Motivar la respuesta. Cuando la ampliación afecte únicamente a la denominación de los modelos o a las versiones referidas en la guía, se hará constar igualmente]*

[Cuando proceda la modificación de la guía, esta se realizará con carácter provisional en el momento de la inclusión y adquirirá carácter definitivo con la publicación del Procedimiento de Empleo Seguro (PES) correspondiente. No es necesario aportar con este documento el texto modificado de la guía.]

8 CONCLUSIONES

La conclusión se formula sobre el impacto de las diferencias analizadas en el apartado 4.

De la conclusión depende el curso del expediente: si las diferencias no impactan en los RFS, la ampliación se resuelve con esta declaración responsable; si impactan, los requisitos relacionados en el apartado 5 deberán verificarse mediante una Evaluación STIC Complementaria antes de ampliar la inclusión.

8.1 CONCLUSIÓN DEL ANÁLISIS

Incluir la conclusión que corresponda:

a) Las diferencias identificadas en el apartado 4 no impactan en los Requisitos Fundamentales de Seguridad de la familia, por lo que no se considera necesaria la realización de una Evaluación STIC Complementaria derivada de las diferencias analizadas.

b) Las diferencias identificadas en el apartado 4 impactan en los Requisitos Fundamentales de Seguridad relacionados en el apartado 5, sobre los modelos, agrupaciones o versiones allí indicados.

Esta conclusión se refiere exclusivamente a las diferencias analizadas en el apartado 4 y no prejuzga la cobertura de los RFS por la declaración de seguridad, que se analiza, cuando proceda, en la JR.

8.2 ENTREGABLES

[Cumplimentar cuando del análisis resulten requisitos afectados.]

El solicitante pondrá a disposición del laboratorio los siguientes elementos:

a) El producto en la configuración correspondiente al alcance solicitado.

b) Los modelos, agrupaciones o versiones sobre los que deba verificarse el alcance pendiente.

c) El entorno de operación necesario para la ejecución de las pruebas.

d) La documentación de instalación y operación aplicable.

9 OBSERVACIONES DEL SOLICITANTE

[Se recoge en este apartado cualquier información adicional que el solicitante considere relevante para la valoración del análisis y que no tenga cabida en los apartados anteriores.]

[Cumplimentar cuando proceda; en otro caso, hacer constar que no existen observaciones.]

10 DECLARACIÓN RESPONSABLE

D./D.ª [nombre y apellidos], con DNI/NIE [documento], en calidad de [cargo] de [organización], en nombre y representación del solicitante, declara bajo su responsabilidad que el contenido del presente documento es cierto y completo y que, en particular:

a) Recoge la totalidad de las diferencias de hardware, firmware y software existentes entre el alcance de partida y el alcance solicitado.

b) Las declaraciones de ausencia de impacto sobre los Requisitos Fundamentales de Seguridad se encuentran técnicamente justificadas y respaldadas por la documentación de producto aportada.

c) Las evidencias referenciadas en el apartado 11 se corresponden con las versiones del producto y de la certificación identificadas en el apartado 2.

d) Los Requisitos Fundamentales de Seguridad no relacionados en el apartado 5 no se ven afectados por las diferencias identificadas.

e) La documentación relacionada en el apartado siguiente se aporta junto a esta declaración responsable o, cuando es pública, se identifica indicando la dirección desde la que resulta accesible.

10.1 DOCUMENTACIÓN APORTADA COMO EVIDENCIA

Se relaciona a continuación la documentación que se aporta como evidencia del análisis, indicando en cada caso si se acompaña a esta declaración responsable o si es pública y desde dónde resulta accesible.

[Incluir una fila por cada documento. La referencia debe coincidir con la empleada en el apartado de referencias.]

Referencia	Documento (título, versión y fecha)	Forma de aportación
[REFn]	*[Título, versión y fecha]*	*[Se aporta junto a esta declaración / Público, accesible en (dirección)]*

Nombre y apellidos	
Cargo	
Organización	
Lugar y fecha	
Firma	*[Espacio reservado para la firma electrónica del responsable técnico del solicitante. No se admiten firmas manuscritas escaneadas.]*

11 REFERENCIAS

Se relacionan las guías y los documentos empleados en la elaboración del análisis. La forma de aportación de las evidencias se indica en el apartado de la declaración responsable.

Referencia	Documento
REF1	CCN-STIC-163 — Guía de procedimiento de inclusión en el CPSMED.
REF2	CCN-STIC-142 — Taxonomía de referencia para productos y servicios médicos conectados (IoMT), Anexo [indicar anexo y familia].
REF3	CCN-STIC-163, Anexo A — Plantilla de Justificación de Requisitos (JR).
REF4	Declaración de seguridad del producto [indicar referencia, versión y fecha].
REF5	Certificado de la evaluación de partida [indicar referencia y fecha].
REF6	Informe técnico de evaluación o informe de certificación [indicar referencia].
REF7	CCN-STIC-807 — Criptología de empleo en el Esquema Nacional de Seguridad.
REF8	Documento de changelog o de detalle de cambios del producto [indicar referencia, versión y fecha].
REF9	Guías de instalación y operación [indicar referencia, versión y fecha].
REF10	Declaración UE de conformidad y, en su caso, certificado del organismo notificado [indicar referencia y fecha].
REF11	[Otras evidencias aportadas].