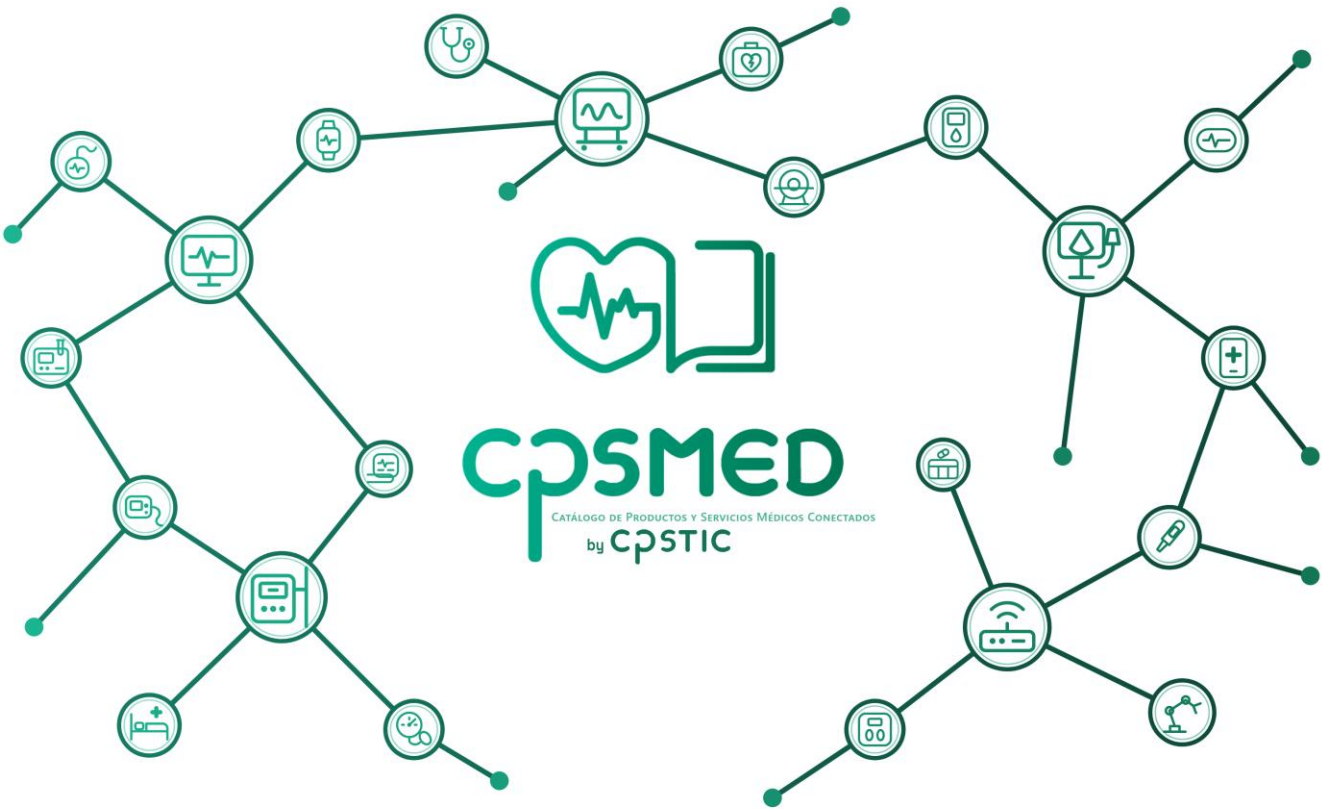
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 163

Procedimiento de inclusión de productos y servicios médicos conectados (IoMT) en el CPSMED



Noviembre 2026

Edita:





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 4
2. OBJETO Y ALCANCE 6
3. TÉRMINOS Y DEFINICIONES 7
3.1 DEFINICIONES 7
3.2 ESTRUCTURA DEL CPSMED 7
3.3 DOCUMENTOS DEL PROCEDIMIENTO DE INCLUSIÓN 8
4. PROCEDIMIENTO DE INCLUSIÓN EN EL CPSMED 11
4.1 INCLUSIÓN INICIAL 12
4.1.1. CERTIFICACIONES ADMITIDAS 12
4.1.2. DOCUMENTACIÓN REGULATORIA DEL PRODUCTO SANITARIO 15
4.1.3. COMPROMISO DE SOPORTE DE SEGURIDAD 15
4.2 RENOVACIÓN DE LA INCLUSIÓN 15
4.3 AMPLIACIÓN DEL ALCANCE DE LA INCLUSIÓN (NUEVAS VERSIONES SOFTWARE O MODELOS HARDWARE) 16
4.3.1. INCLUSIÓN DE NUEVAS VERSIONES 17
4.4 EXPEDIENTES Y PLAZOS DE INCLUSIÓN 17
4.4.1. APERTURA Y VIGENCIA DEL EXPEDIENTE 18
4.4.2. PLAZO DE RESOLUCIÓN DEL TRÁMITE 18
4.4.3. PRÓRROGA EXTRAORDINARIA 18
4.4.4. ARCHIVO DEL EXPEDIENTE Y NUEVA SOLICITUD 18
4.5 FASES DEL PROCEDIMIENTO 19
4.5.1. SOLICITUD DE INCLUSIÓN 19
4.5.2. REVISIÓN DE LA SOLICITUD Y COMUNICACIÓN DE INICIO DE EXPEDIENTE 22
4.5.3. REVISIÓN DE LA PROPUESTA DE DECLARACIÓN DE SEGURIDAD 22
4.5.4. REVISIÓN DE LA CERTIFICACIÓN APORTADA 23
4.5.5. INCLUSIÓN PROVISIONAL Y ENTREGA DEL PROCEDIMIENTO DE EMPLEO SEGURO 24
4.5.6. INCLUSIÓN DEFINITIVA 24
4.5.7. RENOVACIÓN O AMPLIACIÓN DEL ALCANCE 25
5. VIGENCIA Y EXCLUSIÓN DE PRODUCTOS 26
5.1 VIGENCIA DE LA INCLUSIÓN DE PRODUCTOS EN EL CPSMED 26
5.2 PRÓRROGA EXCEPCIONAL DE LA VIGENCIA 26
5.3 EXCLUSIÓN DEL CPSMED 26
6. DISTINTIVO DE INCLUSIÓN 27
6.1 CONDICIONES DE USO 27
6.2 DISTINTIVO DE PRODUCTO INCLUIDO EN EL CPSMED 27
7. REFERENCIAS 28
8. ABREVIATURAS 30

1. INTRODUCCIÓN

La adquisición de un producto sanitario conectado (IoMT, Internet of Medical Things) que va a tratar información de la salud de los pacientes, o cuyo funcionamiento incide directamente en su propia seguridad, debe estar precedida de un proceso de comprobación de que los mecanismos de seguridad implementados en el producto son adecuados para proteger dicha información y garantizar la continuidad de la asistencia sanitaria.

La evaluación y certificación de la seguridad de un producto por un tercero independiente es el medio más objetivo para valorar y acreditar su capacidad para proteger la información que trata y mantener de forma segura las funciones de las que depende la asistencia al paciente. 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.*

El ENS no regula los productos sanitarios como tales, pero estos forman parte de los sistemas de información a los que se aplica: los de los centros y servicios sanitarios del sector público y los de las entidades privadas que les prestan servicios mediante

contrato, convenio o encomienda, como los centros concertados (artículo 2). Su compromiso puede afectar a la confidencialidad de los datos de salud, a la integridad de la información en la que se basan las decisiones clínicas, a la disponibilidad de la asistencia y, en último término, a la seguridad del paciente. Aunque el artículo 19 se refiere a los productos de seguridad, el ENS aplica el mismo criterio a los equipos conectados mediante sus medidas de seguridad: la medida op.pl.5 *Componentes certificados* desarrolla dicho artículo, y la medida mp.eq.4 *Otros dispositivos conectados a la red* pide, en su refuerzo R1, emplear productos certificados siempre que sea posible.

El perfil de cumplimiento específico para el sector salud, guía CCN-STIC-891 [3], es el único documento del ENS que trata expresamente los equipos médicos. Indica que la medida mp.eq.4 se centrará especialmente en los dispositivos médicos conectados a la red y en el IoMT (apartado 4.9) y que, en los equipos médicos, exigir componentes certificados probablemente requerirá medidas compensatorias, como otra certificación o una acreditación de producto reconocida en el sector (apartado 4.3). El CPSMED responde a esa necesidad: los productos incluidos tienen certificada su funcionalidad de seguridad frente a los requisitos que el CCN define para cada familia en la CCN-STIC-142.

Por su parte, los productos sanitarios están sujetos al Reglamento (UE) 2017/745 sobre los productos sanitarios (MDR) [4] y al Reglamento (UE) 2017/746 sobre los productos sanitarios para diagnóstico in vitro (IVDR) [5], desarrollados en España por el Real Decreto 192/2023 [6], que exigen a los fabricantes tener en cuenta la seguridad de la información en el diseño y la fabricación de sus productos. La inclusión de un producto en el catálogo no sustituye al marcado CE ni a la evaluación de la conformidad prevista en dicha normativa, sino que la complementa, valorando de forma específica las funcionalidades de seguridad del producto.

En virtud de estas competencias, el CCN publica la guía CCN-STIC-162 Catálogo de Productos y Servicios Médicos Conectados (CPSMED) [7], cuya finalidad es ofrecer a los organismos de la Administración, y en particular a los centros y servicios sanitarios, un conjunto de productos y servicios médicos conectados de referencia cuyas funcionalidades de seguridad han sido certificadas, y la guía CCN-STIC-142 Taxonomía de referencia para productos y servicios médicos conectados (IoMT) [8], que clasifica dichos productos en categorías y familias y define, en sus anexos, los Requisitos Fundamentales de Seguridad (RFS) exigibles a cada familia.

2. OBJETO Y ALCANCE

El objeto de la presente guía es definir el procedimiento y las evaluaciones requeridas para incluir un producto sanitario conectado en el CPSMED [7], así como las condiciones de vigencia, renovación, ampliación del alcance y exclusión de los productos incluidos.

El procedimiento es de aplicación a los productos sanitarios conectados clasificados conforme a la taxonomía CCN-STIC-142 [8], tanto si se presentan como dispositivo dedicado (hardware con su firmware y software) como si se trata de software instalado y operado en la infraestructura del propio centro sanitario o en el dispositivo del paciente.

Quedan fuera del alcance de la presente guía: los productos desplegados en nube y prestados como servicio (SaaS, PaaS o IaaS), cuyo procedimiento de inclusión será objeto de desarrollo específico; los dispositivos conectados sin finalidad médica; los productos de bienestar sin marcado CE como producto sanitario; los productos de seguridad TIC destinados a proteger los entornos IoMT, que se rigen por el CPSTIC [9], y los productos y servicios de conformidad y gobernanza, que no forman parte del CPSMED. No obstante, sí podrán incluirse los dispositivos en los que parte del TOE se encuentre desplegada en la nube (por ejemplo, una aplicación o un servicio de gestión remota), en las condiciones del apartado 4.1.1.

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 sanitario conectado: producto que tiene la consideración de producto sanitario conforme al MDR [4], o de producto sanitario para diagnóstico in vitro conforme al IVDR [5], y que dispone de capacidades de comunicación, cableadas o inalámbricas, con otros dispositivos, redes o sistemas de información. Se incluyen el software que es producto sanitario por sí mismo y los accesorios y elementos de conectividad que forman parte del sistema del producto sanitario, así como el software de gestión del centro sanitario contemplado en la familia Software de gestión de la CCN-STIC-142 [8].

Finalidad prevista: uso al que se destina el producto según los datos facilitados por el fabricante en el etiquetado, las instrucciones de uso y la documentación técnica, conforme al MDR. Determina la familia o familias de la taxonomía en las que se encuadra el producto.

Familia y criticidad: agrupación de productos de la taxonomía CCN-STIC-142 atendiendo a su función clínica básica. Cada familia tiene asignada una criticidad orientativa (ALTA, MEDIA o BÁSICA) que refleja el impacto potencial de un compromiso de la seguridad de sus productos sobre el paciente y la asistencia; la criticidad no modifica los RFS exigibles.

Certificación reconocida: certificación de seguridad admitida para la inclusión en el CPSMED conforme al apartado 4.1.1: Certificación Nacional Esencial de Seguridad (LINCE), certificación Common Criteria, certificación UL 2900-2-1 o, cuando el anexo de la familia lo contemple, una certificación específica de la familia (por ejemplo, IEEE 2621 para la familia Dispositivos de insulina).

Requisitos Fundamentales de Seguridad (RFS): requisitos mínimos de seguridad que debe cumplir en su totalidad un producto para ser incluido en el CPSMED. Se definen para cada familia en los anexos de la guía CCN-STIC-142 [8], junto con el problema de seguridad (hipótesis sobre el entorno, activos y amenazas) frente al que deben evaluarse.

3.2 ESTRUCTURA DEL CPSMED

El CPSMED se compone de un único listado de productos incluidos. No distingue entre productos aprobados y cualificados, ni establece distintos niveles de requisitos. La inclusión responde a un criterio único de todo o nada:

a) El producto debe cumplir la totalidad de los RFS definidos para la familia o familias de la CCN-STIC-142 en las que se encuadra, determinadas por su finalidad prevista.

b) El incumplimiento de cualquiera de ellos impide su inclusión en el CPSMED; no existen inclusiones parciales ni por niveles.

c) Cuando un producto se encuadre en varias familias complementarias, deberá cumplir los RFS de todas ellas.

La Figura 1 representa la estructura del CPSMED y las guías que intervienen en el procedimiento de inclusión.



Figura 1. Estructura del CPSMED y guías aplicables

Los RFS exigibles a cada familia, junto con el problema de seguridad frente al que deben evaluarse, los casos de uso contemplados y las certificaciones reconocidas para la familia, se detallan en los anexos de la guía CCN-STIC-142 [8] (por ejemplo, Anexo A.1 Dispositivos de insulina [10] y Anexo A.2 Bombas inteligentes [11]). Para las familias cuyo anexo no se haya publicado, el solicitante podrá pedir al CCN que defina los requisitos aplicables. El CCN los comunicará por escrito antes de iniciar la evaluación, y se tendrán en cuenta en la elaboración del anexo de la familia.

Un producto incluido en el CPSMED hará referencia a una versión concreta (hardware, firmware y software) y a una configuración determinada, definida en un Procedimiento de Empleo Seguro (PES). El PES será distribuido por el fabricante junto con el producto y se publicará como una guía CCN-STIC de la serie 4000, que se referenciará en la información contenida en el CPSMED. El PES recogerá también las medidas que corresponde aplicar a la organización sanitaria durante el despliegue y la operación del producto (por ejemplo, la segmentación de la red clínica conforme a IEC 80001-1 [12]), ya que estas no forman parte de los RFS del producto.

3.3 DOCUMENTOS DEL PROCEDIMIENTO DE INCLUSIÓN

En el proceso de inclusión intervienen los documentos que se relacionan en la Tabla 1, 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-CPSMED-02) y declaración responsable (FOR-CPSMED-01)	Solicitante	Formularios publicados en la web del CPSMED
Declaración de Seguridad (DS) — LINCE o Common Criteria	Solicitante	Metodología de certificación de origen

Documento	Elabora	Contenido definido en
Declaración de Seguridad (DS) — Evaluación STIC Complementaria	Solicitante	CCN-STIC-2003 [13]
Certificado e informe de certificación — UL 2900-2-1 o certificación específica de la familia	Solicitante	Norma de certificación de origen
Resultados de las pruebas sobre los componentes de IA o desplegados en la nube (cuando el CCN las exija)	Solicitante	Las que determine el CCN (apartado 4.1.1)
Justificación de Requisitos (JR)	Solicitante	Anexo A de la presente guía [14]
Informe de Análisis Diferencial (IAD)	Solicitante	Anexo B de la presente guía [15]
Procedimiento de Empleo Seguro (PES)	Solicitante	Anexo C de la presente guía [16]
Documentación regulatoria del producto sanitario (declaración UE de conformidad, certificado del organismo notificado, instrucciones de uso)	Fabricante	MDR / IVDR
Documentación técnica de ciberseguridad (análisis de riesgos de seguridad, SBOM y, en su caso, formulario MDS2)	Fabricante	MDR / IVDR, Anexos I y II
Plan de evaluación	Laboratorio	Validado por el CCN en cada expediente
Informe Técnico de Evaluación (ITE)	Laboratorio	CCN-STIC-2004 [17]
COM-INI, RRPDS, ITI y RITI	CCN	Apartado 4.5

Tabla 1. Documentos que intervienen en el procedimiento

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

EXPEDIENTE DE INCLUSIÓN · Productos y servicios médicos conectados Apartado 4	
Trámites	Inclusión inicial · Renovación · Ampliación del alcance (series y versiones)
Garantía exigida	Certificación reconocida en vigor admitida para la familia: LINCE, Common Criteria, UL 2900-2-1 o certificación propia del tipo de dispositivo reconocida en el anexo de la familia (apartado 4.1.1) Producto sin certificación: obtener, a elección del solicitante, una certificación LINCE, Common Criteria, UL 2900-2-1 o la certificación propia reconocida en el anexo de la familia (apartado 4.5.3) RFS no cubiertos: Evaluación STIC Complementaria (apartado 4.1.1.1) Productos con inteligencia artificial integrada o con parte del TOE en la nube: declaración en la solicitud (FOR-CPSMED-02) y pruebas que determine el CCN (apartado 4.1.1) Compromiso de soporte de seguridad durante 5 años desde la inclusión, asumido en la declaración responsable FOR-CPSMED-01 (apartado 4.1.3)
Evidencias	Certificación y DS o informe de certificación (sin certificación: la que se pretende obtener y la propuesta de DS o del alcance previsto) · descripción de los componentes de IA o en la nube (si los hay) · JR · política de versionado · documentación regulatoria (4.1.2) IAD en las ampliaciones del alcance
Vigencia	Expediente: hasta 5 años de antigüedad de la certificación Inclusión: 2 años o hasta el fin de soporte de seguridad, lo que ocurra antes · renovable mediante solicitud de renovación

Figura 2. Tipos de trámite y condiciones aplicables a la inclusión en el CPSMED

4. PROCEDIMIENTO DE INCLUSIÓN EN EL CPSMED

Este apartado describe el procedimiento de inclusión de productos sanitarios conectados en el CPSMED. La Figura 3 representa el procedimiento.

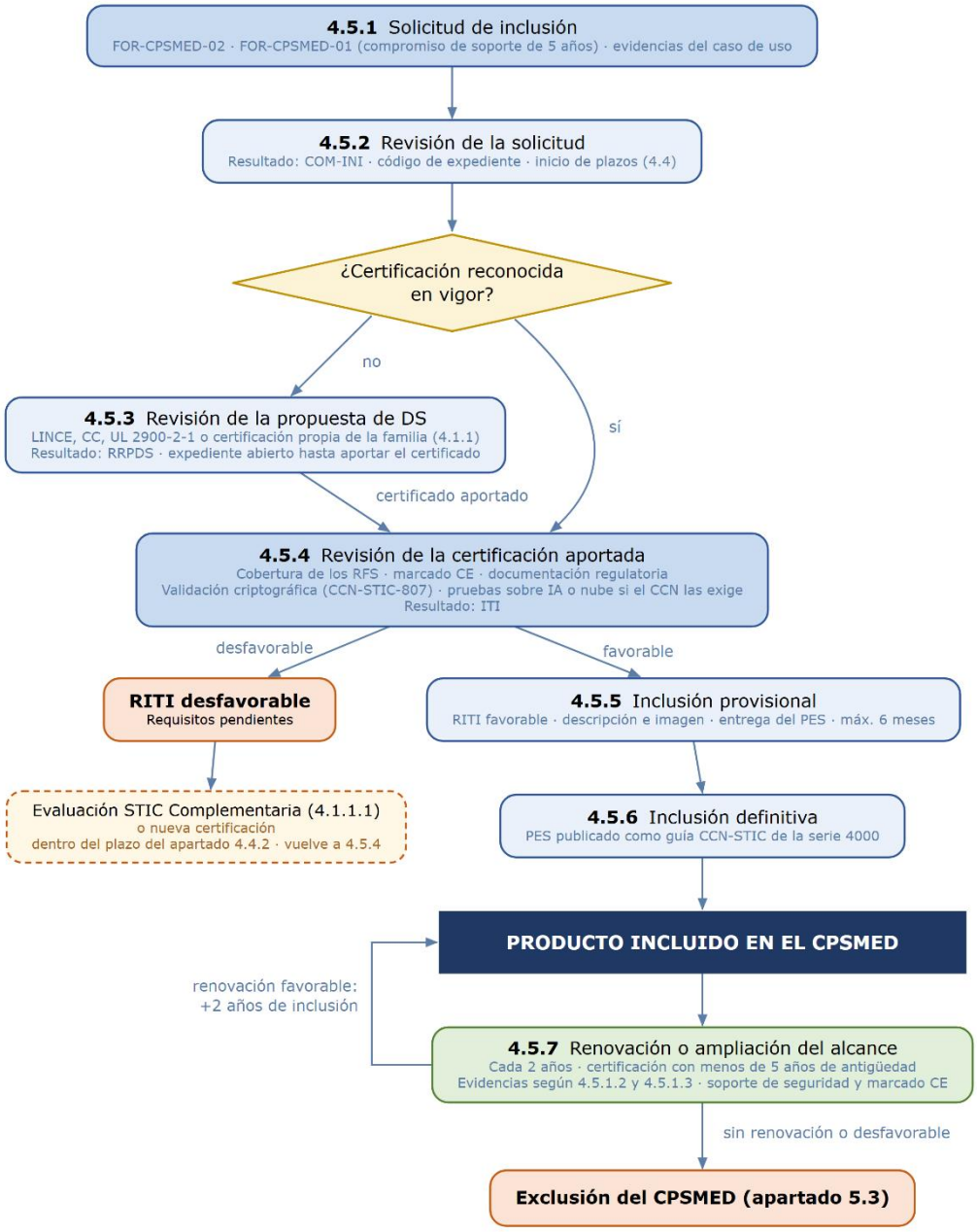


Figura 3. Procedimiento de inclusión en el CPSMED

El solicitante deberá indicar en la solicitud de inclusión en qué familia o familias encaja el producto, de acuerdo con la taxonomía establecida en la guía CCN-STIC-142 [8] y con la finalidad prevista declarada por el fabricante, dado que de ellas dependen los RFS exigibles y las evidencias asociadas. Cuando el producto se encuadre en varias familias, deberá acreditar el cumplimiento de los RFS de todas ellas.

En caso de que el producto no encaje en ninguna familia de las contempladas en la taxonomía, o de que el anexo de RFS de su familia no se haya publicado todavía, el solicitante lo hará constar en la solicitud. El CCN estudiará individualmente dichas solicitudes y determinará, caso por caso, qué requisitos de seguridad deberá implementar y certificar el producto.

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 cuando la familia indicada no se corresponda con la finalidad prevista del producto o cuando no se solicite la inclusión de su función clínica principal.

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

d) Excluir del catálogo los productos multifunción cuando el solicitante haga publicidad engañosa acerca de las funcionalidades incluidas en el CPSMED.

Dentro de este procedimiento se distinguen tres tipos de trámites:

a) Inclusión inicial.

b) Renovación de la inclusión.

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

4.1 INCLUSIÓN INICIAL

La inclusión inicial en el CPSMED exige acreditar una certificación reconocida por el CCN que cubra la totalidad de los RFS de la familia o familias del producto, evaluados considerando el problema de seguridad definido en el anexo correspondiente de la CCN-STIC-142. En este apartado se definen las certificaciones admitidas y la forma de completar su cobertura cuando no alcance a todos los RFS.

4.1.1. CERTIFICACIONES ADMITIDAS

Para que un producto pueda ser incluido en el CPSMED deberá disponer de una certificación reconocida, en vigor y emitida sobre la versión y los modelos que se pretenden incluir. Si no dispone de ella al presentar la solicitud, deberá obtener, a su elección, una certificación LINCE, Common Criteria, UL 2900-2-1 o la certificación propia que reconozca el anexo de su familia durante la tramitación del expediente (apartado 4.5.3). Las certificaciones admitidas para cada familia se concretan en su anexo de RFS de la CCN-STIC-142 y son las siguientes:

a) Certificación Nacional Esencial de Seguridad (LINCE) [18], válida para cualquier familia de la taxonomía.

b) Certificación Common Criteria, con el nivel de confianza (EAL, Evaluation Assurance Level) determinado por el perfil de protección cuando el producto

se encuentre certificado contra alguno, o EAL2 o superior en caso contrario, válida para cualquier familia de la taxonomía.

c) Certificación UL 2900-2-1, emitida por un organismo de certificación acreditado, que acredite la conformidad del producto con la norma ANSI/CAN/UL 2900-1 y con los requisitos particulares de la norma UL 2900-2-1 para componentes conectables a red de sistemas sanitarios [19]. Por su carácter general para los productos sanitarios conectados, esta certificación es válida para cualquier familia de la taxonomía.

d) Certificación específica de la familia: las certificaciones propias del tipo de dispositivo que el anexo de RFS de la familia reconozca expresamente, válidas únicamente para dicha familia. Es el caso de la certificación IEEE 2621 [20] para la familia Dispositivos de insulina, emitida en el marco del programa de certificación de IEEE conforme a la norma IEEE 2621.1, que acredite la conformidad del producto con la norma IEEE 2621.2 con un paquete de garantía Enhanced-basic o Moderate [10].

La certificación aportada deberá incluir los RFS de la familia, evaluados considerando el problema de seguridad (hipótesis sobre el entorno, activos y amenazas) definido en el anexo correspondiente de la CCN-STIC-142. Dado el criterio de todo o nada del catálogo, no se admitirán inclusiones parciales: todos los RFS deberán quedar acreditados, ya sea por la certificación aportada o por una Evaluación STIC Complementaria.

En el caso de que la certificación aportada no incluya todos los RFS definidos para la familia, pero el producto sí implemente las funciones de seguridad correspondientes, deberá completarse el proceso realizando una Evaluación STIC Complementaria como la descrita en el apartado 4.1.1.1.

Cuando el producto integre sistemas o componentes de inteligencia artificial (IA), o cuando parte del TOE se encuentre desplegada en la nube (por ejemplo, una aplicación o un servicio de gestión remota), el solicitante deberá declararlo en la solicitud de inclusión (FOR-CPSMED-02). En estos casos, el CCN se reserva la potestad de exigir, sobre dichos componentes, las pruebas o evaluaciones que correspondan o que considere oportunas, en cualquiera de los trámites de inclusión.

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 [18] y CCN-STIC-2002 [21]), 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.

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 [13] 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 de partida, completadas con las definidas en el anexo de la familia de la CCN-STIC-142.

El resultado se recogerá en el Informe Técnico de Evaluación (**ITE**), elaborado conforme a la plantilla de la CCN-STIC-2004 [17].

4.1.1.2. TRAZABILIDAD DE LA CERTIFICACIÓN APORTADA CON LOS RFS

Para determinar qué RFS quedan cubiertos por la certificación aportada y cuáles deben verificarse mediante una Evaluación STIC Complementaria, se tendrán en cuenta las siguientes reglas:

a) Certificaciones LINCE: los anexos de RFS de la CCN-STIC-142 indican qué funciones de seguridad se consideran aplicables en una certificación LINCE; la DS deberá recoger los RFS correspondientes.

b) Certificaciones UL 2900-2-1 o específicas de la familia: los anexos de RFS incluyen tablas de trazabilidad entre los RFS y los requisitos o apartados de la norma correspondiente (por ejemplo, la trazabilidad con IEEE 2621 del Anexo A.1 o con UL 2900-2-1 del Anexo A.2). Las celdas vacías de dichas tablas suponen que la norma no incluye un requisito que satisfaga el RFS, que deberá verificarse en la Evaluación STIC Complementaria.

c) Cuando el anexo de la familia no incluya tabla de trazabilidad para la certificación aportada, en particular en el caso de la certificación UL 2900-2-1, el solicitante justificará la equivalencia entre los requisitos certificados y los RFS en la Justificación de Requisitos (JR) conforme al Anexo A de la presente guía [14], y el CCN la validará.

d) La equivalencia dependerá de las asignaciones y selecciones realizadas en la certificación aportada; los requisitos opcionales de la norma solo cubrirán el RFS correspondiente cuando se hayan incluido en el alcance de la certificación, y las prácticas recomendadas, solo cuando se haya acreditado su cumplimiento.

La equivalencia de requisitos deberá ser justificada por el solicitante y validada por el CCN en la fase de revisión de la certificación (apartado 4.5.4).

4.1.2. DOCUMENTACIÓN REGULATORIA DEL PRODUCTO SANITARIO

Además de la certificación de seguridad, el solicitante deberá acreditar que el producto dispone de marcado CE como producto sanitario conforme al MDR o al IVDR para la finalidad prevista declarada, aportando la siguiente documentación:

a) La declaración UE de conformidad y, cuando proceda, el certificado emitido por el organismo notificado.

b) Las instrucciones de uso y la documentación técnica de ciberseguridad del producto: análisis de riesgos de seguridad, lista de componentes software (SBOM) y, en su caso, el formulario de divulgación de seguridad del fabricante (MDS2).

Cuando un producto se comercialice tanto en una versión con finalidad médica como en otra sin ella, únicamente la primera podrá ser incluida en el CPSMED. Los productos que integren sistemas de inteligencia artificial deberán acreditar, además, el cumplimiento de los requisitos del Reglamento (UE) 2024/1689 [22] para los sistemas de alto riesgo, sin perjuicio de las pruebas que el CCN pueda exigir conforme al apartado 4.1.1.

4.1.3. COMPROMISO DE SOPORTE DE SEGURIDAD

El solicitante deberá comprometerse, en la declaración responsable (FOR-CPSMED-01), a mantener el soporte de seguridad de la versión y de los modelos del producto incluidos en el CPSMED durante un periodo mínimo de cinco (5) años desde la fecha de inclusión del producto en el catálogo, con independencia de que se siga comercializando o no.

El fabricante notificará al CPSMED cualquier circunstancia que pueda afectar a dicho compromiso. Su incumplimiento será motivo de exclusión del catálogo (apartado 5.3).

4.2 RENOVACIÓN DE LA INCLUSIÓN

Cuando un producto es incluido en el CPSMED, se le asigna una “fecha de revisión de validez” que, como máximo, será de dos (2) años desde la inclusión inicial. Como su propio nombre indica, esta será la fecha en la que el solicitante y el equipo del CPSMED 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 CPSMED, sigue teniendo soporte de seguridad, independientemente de si se sigue comercializando o no.

b) La certificación aportada para la inclusión 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.

d) El producto mantiene el marcado CE como producto sanitario para la finalidad prevista declarada y no ha sido objeto de retirada del mercado.

e) Cuando el producto integre inteligencia artificial o parte del TOE se encuentre desplegada en la nube, se han superado las pruebas que, en su caso, haya exigido el CCN sobre dichos componentes (apartado 4.1.1).

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

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

Las certificaciones reconocidas para la inclusión en el CPSMED (LINCE, Common Criteria, UL 2900-2-1 o específicas de la familia) aplican únicamente a la versión o versiones del producto y a los modelos hardware especificados en la declaración de seguridad o en el alcance de la certificación.

Para la inclusión de versiones software/firmaware posteriores a una certificada o de 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 inclusión 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.

c) Los cambios constituyen un cambio significativo del producto sanitario que, conforme al MDR, requiera una nueva evaluación de la conformidad por parte del organismo notificado, en tanto no se aporte el certificado actualizado.

La Tabla 2 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 incluir.

Tabla 2. Términos empleados en la ampliación a 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 [15], 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 incluir 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.

En el caso de aplicaciones software que forman parte del producto y se ejecutan sobre dispositivos móviles de consumo, el IAD deberá contemplar además los cambios en las versiones de sistema operativo y en las plataformas móviles compatibles declaradas por el fabricante.

4.4 EXPEDIENTES Y PLAZOS DE INCLUSIÓN

El expediente es la unidad de tramitación que vincula un producto con su proceso de inclusión en el CPSMED. Bajo un mismo expediente se realizan todos los trámites relativos a un producto 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 inclusión 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) **Para las certificaciones UL 2900-2-1 o específicas de la familia, el periodo de validez que establezca el programa de certificación correspondiente, con un máximo de cinco (5) años.**

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.

El expediente se cerrará cuando la certificación que lo sustenta pierda su vigencia o alcance los cinco (5) años de antigüedad, momento en el que se dejarán de admitir renovaciones y ampliaciones del alcance.

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 5.2, 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 3.

4.5.1. SOLICITUD DE INCLUSIÓN

Documentos de entrada: los formularios FOR-CPSMED-02 y FOR-CPSMED-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 (cpsmed@ccn.cni.es) de la solicitud de inclusión en el CPSMED, cumplimentando los siguientes formularios, disponibles en la web del CPSMED (https://cpsmed.ccn.cni.es):

- **FOR-CPSMED-02** — Solicitud de inclusión en el Catálogo de Productos y Servicios Médicos Conectados (CPSMED).
- **FOR-CPSMED-01** — Declaración responsable para la inclusión en el Catálogo de Productos y Servicios Médicos Conectados (CPSMED), en la que el solicitante asume, entre otros, el compromiso de mantener el soporte de seguridad del producto durante cinco (5) años desde su inclusión en el catálogo (apartado 4.1.3).

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

4.5.1.1. INCLUSIÓN INICIAL

Aplicable cuando se pretende incluir por primera vez un producto y una versión concretos en el CPSMED, 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 con certificación en vigor. Junto a la solicitud se adjuntará:

a) **La certificación reconocida** (LINCE, Common Criteria, UL 2900-2-1 o específica de la familia), junto con su Declaración de Seguridad (DS) o, en su caso, el informe de certificación que identifique su alcance.

b) Cuando el producto integre inteligencia artificial o parte del TOE se encuentre desplegada en la nube, la descripción de dichos componentes, conforme a lo declarado en la solicitud (apartado 4.1.1). El CCN comunicará, en su caso, las pruebas que deban realizarse sobre ellos.

c) **Justificación de Requisitos (JR**), conforme a la plantilla del Anexo A de la presente guía [14], siempre y cuando existan diferencias entre los RFS definidos para la familia solicitada y los cubiertos por la certificación, o cuando el anexo de la familia no incluya tabla de trazabilidad para la certificación aportada.

d) **Informe de Análisis Diferencial (IAD)**, conforme a la plantilla del Anexo B de la presente guía [15], cuando la versión o los modelos que se pretenden incluir no coincidan con los recogidos en la certificación aportada.

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

f) 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 [16].

g) La documentación regulatoria del producto sanitario descrita en el apartado 4.1.2.

Producto sin certificación en vigor. El producto aún no dispone de una certificación reconocida y deberá obtener, a su elección, una certificación LINCE, Common Criteria, UL 2900-2-1 o la certificación propia que reconozca el anexo de su familia (apartado 4.1.1). Junto a la solicitud se adjuntará:

a) La certificación que se pretende obtener y la propuesta de Declaración de Seguridad (DS) con la que se pretende certificar el producto o, cuando el esquema elegido no contemple una DS, la definición del alcance previsto de la certificación, 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 [14].

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 [16].

e) La documentación regulatoria del producto sanitario descrita en el apartado 4.1.2 o, si el producto se encuentra en proceso de evaluación de la conformidad, el estado de dicho proceso. La inclusión no se hará efectiva hasta que el producto disponga de marcado CE.

f) Cuando el producto integre inteligencia artificial o parte del TOE se encuentre desplegada en la nube, la descripción de dichos componentes, conforme a lo declarado en la solicitud (apartado 4.1.1). Los resultados de las pruebas que, en su caso, exija el CCN sobre ellos podrán aportarse junto con el certificado.

Emitido el RRPDS, el expediente permanecerá abierto hasta que el solicitante aporte el certificado emitido conforme al esquema elegido, 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).

4.5.1.2. RENOVACIÓN

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

A tal efecto, bastará con presentar la solicitud (FOR-CPSMED-02) marcando la opción de renovación y aportar la evidencia de que el producto mantiene soporte de seguridad y marcado CE: 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. Cuando el producto integre inteligencia artificial o parte del TOE se encuentre desplegada en la nube, se declararán, además, los cambios en dichos componentes desde la última revisión, y el CCN podrá exigir sobre ellos las pruebas que considere oportunas (apartado 4.1.1).

4.5.1.3. AMPLIACIÓN DEL ALCANCE

Aplicable cuando se pretende ampliar el alcance de la inclusión a una nueva versión del producto o a nuevos modelos de una serie, partiendo de la certificación y de la inclusión existentes. La ampliación actualiza la fecha de la revisión de la inclusión (apartado 5.1).

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 [15]. 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) Cuando los cambios afecten a los componentes de inteligencia artificial o desplegados en la nube, su descripción; el CCN podrá exigir sobre ellos las pruebas que considere oportunas (apartado 4.1.1).

d) 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 reconocida.

4.5.1.4. RESUMEN DE EVIDENCIAS POR CASO DE USO

La Tabla 3 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 · producto con certificación en vigor	Solicitud (FOR-CPSMED-02/01), certificación reconocida y DS o informe de certificación, JR (según caso), documentación regulatoria (4.1.2), descripción de los componentes de IA o en la nube, si los hay, 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 de la familia; si no los cubre en su totalidad, Evaluación STIC Complementaria (4.1.1.1).

Caso de uso	Documentación a aportar	Fases y evaluación aplicables
Inclusión inicial · producto sin certificación en vigor	Solicitud, certificación que se pretende obtener y propuesta de DS o del alcance previsto, JR, política de versionado y documentación regulatoria (4.1.2); descripción de los componentes de IA o en la nube, si los hay.	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.
Renovación	Solicitud (FOR-CPSMED-02), evidencia de soporte de seguridad y de marcado CE vigentes; cambios en los componentes de IA o en la nube, si los hay; 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), de soporte de seguridad y de marcado CE; renueva 2 años o hasta el fin de soporte, lo que ocurra antes.
Ampliación del alcance · series de productos	Solicitud, DS de partida, IAD con matriz de características, descripción de los cambios en los componentes de IA o en la nube, si los hay, 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, descripción de los cambios en los componentes de IA o en la nube, si los hay, 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.

Tabla 3. 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 reconocida en vigor.

Documentos de entrada: la propuesta de Declaración de Seguridad o, en su caso, del alcance previsto de la certificación, 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 o del alcance previsto de la certificación y la Justificación de Requisitos frente a los RFS de la familia o familias declaradas y frente al problema de seguridad definido en el anexo correspondiente de

la CCN-STIC-142, 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 propuesta, 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 APORTADA

Documentos de entrada: la certificación reconocida y su declaración de seguridad o informe de certificación, la Justificación de Requisitos cuando proceda, la documentación regulatoria del producto sanitario, la descripción de los componentes de inteligencia artificial o desplegados en la nube y los resultados de las pruebas que, en su caso, haya exigido el CCN sobre ellos, el listado de algoritmos criptográficos empleados y las evidencias complementarias que el CCN requiera.

El CCN verifica en esta fase que la certificación aportada cubre la totalidad de los RFS de la familia o familias solicitadas, aplicando, en su caso, las tablas de trazabilidad del anexo correspondiente de la CCN-STIC-142 o la equivalencia justificada en la JR, y que el producto dispone de marcado CE para la finalidad prevista declarada. Cuando el producto integre inteligencia artificial o parte del TOE se encuentre desplegada en la nube, el CCN verificará, además, los resultados de las pruebas que haya exigido sobre dichos componentes (apartado 4.1.1).

Si la certificación cubre todos los RFS exigibles, el CCN realizará una revisión básica, sin evaluaciones adicionales en laboratorio salvo las pruebas que haya exigido sobre los componentes de IA o desplegados en la nube, emitirá un Informe Técnico de Inclusión (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.

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 en la guía CCN-STIC-807 [23].

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 CPSMED, 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 [16].

La propuesta se remitirá, en formato editable y respetando la estructura y los estilos de dicha plantilla, a la dirección cpsmed@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.

El PES recogerá también las medidas que corresponde aplicar a la organización sanitaria durante el despliegue y la operación del producto, conforme al apartado correspondiente del Anexo C.

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

Resultado: inclusión provisional del producto en el CPSMED. 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 4000. El fabricante distribuirá el PES junto con el producto.

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 5.1.

Toda ampliación del alcance o nueva versión incluida 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 4000 e inclusión definitiva del producto en el CPSMED.

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 inclusión 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-CPSMED-02) indicando la modalidad: renovación de la inclusión 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) Aporta, asimismo, la evidencia de que el producto mantiene el marcado CE para la finalidad prevista declarada y, cuando integre inteligencia artificial o parte del TOE se encuentre desplegada en la nube, declara los cambios en dichos componentes.

d) El CCN verifica que la certificación reconocida tiene una antigüedad inferior a cinco (5) años y que se mantienen el soporte de seguridad y el marcado CE. Sobre los componentes de IA o desplegados en la nube, podrá exigir las pruebas que considere oportunas (apartado 4.1.1).

e) 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.

f) Si existe una Evaluación STIC Complementaria o una certificación en curso, se aplicará la prórroga excepcional de tres (3) meses (apartado 5.2).

Alcanzada la fecha de revisión de validez sin que se produzca la renovación o la ampliación, el producto será excluido del CPSMED conforme al apartado 5.3.

Resultado: renovación o ampliación del alcance de la inclusión.

5. VIGENCIA Y EXCLUSIÓN DE PRODUCTOS

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

5.1 VIGENCIA DE LA INCLUSIÓN DE PRODUCTOS EN EL CPSMED

La inclusión en el CPSMED tiene una vigencia de dos (2) años o hasta la fecha de fin de soporte de seguridad declarada por el fabricante, lo que ocurra antes. Las particularidades de la renovación y de la ampliación del alcance se detallan en los apartados 4.5.1.2, 4.5.1.3 y 4.5.7. La Tabla 4 resume dichas condiciones.

Ámbito	Vigencia	Renovación / ampliación
Productos incluidos en el CPSMED	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 y marcado CE (con evidencia) y la certificación reconocida tiene menos de 5 años. Si el producto integra IA o tiene parte del TOE en la nube, el CCN podrá exigir las pruebas que considere oportunas sobre esos componentes.

Tabla 4. Vigencia de la inclusión en el CPSMED

5.2 PRÓRROGA EXCEPCIONAL DE LA VIGENCIA

La validez de la inclusión podrá ampliarse excepcionalmente tres (3) meses adicionales cuando el fabricante haya iniciado un proceso de renovación o de ampliación del alcance que requiera una Evaluación STIC Complementaria o una nueva certificación, con el fin de dar tiempo a que dicho proceso finalice.

5.3 EXCLUSIÓN DEL CPSMED

Un producto podrá ser excluido del CPSMED por cualquiera de los siguientes motivos:

- Alcance de la fecha de vigencia (dos años o 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 la certificación reconocida aportada. Para las certificaciones 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, o si puede comprometer la seguridad del paciente, la entrada será excluida.
- **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 CPSMED, o incumplimiento del compromiso de mantener el soporte de seguridad durante cinco (5) años desde la inclusión (apartado 4.1.3).
- Resultado desfavorable de la revisión periódica de las evidencias.
- Pérdida, suspensión o retirada del marcado CE del producto, retirada del producto del mercado o modificación de su finalidad prevista que lo sitúe fuera del alcance de la taxonomía.
- Emisión de una acción correctiva de seguridad en campo (FSCA) o de un aviso de seguridad que afecte a las funciones de seguridad del producto, cuando el fabricante no acredite su corrección en el plazo que determine el CCN.

6. DISTINTIVO DE INCLUSIÓN

6.1 CONDICIONES DE USO

La inclusión de un producto en el CPSMED podrá representarse mediante el distintivo de inclusión expedido por el CCN. Su uso queda condicionado a la inclusión en el CPSMED. El solicitante podrá, de forma voluntaria, dar publicidad a los productos incluidos exhibiendo el distintivo en su documentación técnica o comercial, en cualquier formato. El distintivo vigente se encontrará en la sección «MEDIA» de la web del CPSMED (https://cpsmed.ccn.cni.es).

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 CPSMED (apartado 5.3), el solicitante deberá retirar los distintivos empleados en su documentación.

6.2 DISTINTIVO DE PRODUCTO INCLUIDO EN EL CPSMED

Corresponde a los productos incluidos en el CPSMED. Al no existir categorías ni niveles de inclusión, se emplea un único distintivo, que presenta el aspecto siguiente.



Figura 4. Distintivo de producto incluido en el CPSMED

7. 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-891 Perfil de Cumplimiento Específico para Salud. Prestación sanitaria a pacientes: Atención Primaria y Atención Especializada (febrero de 2024).

[4] Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios (MDR).

[5] Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios para diagnóstico in vitro (IVDR).

[6] Real Decreto 192/2023, de 21 de marzo, por el que se regulan los productos sanitarios.

[7] CCN-STIC-162 Catálogo de Productos y Servicios Médicos Conectados (CPSMED).

[8] CCN-STIC-142 Taxonomía de referencia para productos y servicios médicos conectados (IoMT) y sus anexos.

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

[10] Anexo A.1 CCN-STIC-142 Requisitos Fundamentales de Seguridad – Dispositivos de insulina.

[11] Anexo A.2 CCN-STIC-142 Requisitos Fundamentales de Seguridad – Bombas de infusión inteligentes.

[12] IEC 80001-1:2021 Application of risk management for IT-networks incorporating medical devices – Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software.

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

[14] Anexo A CCN-STIC-163 Plantilla de Justificación de Requisitos (JR).

[15] Anexo B CCN-STIC-163 Plantilla de Informe de Análisis Diferencial (IAD).

[16] Anexo C CCN-STIC-163 Plantilla de Procedimiento de Empleo Seguro (PES).

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

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

[19] ANSI/CAN/UL 2900-1 Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, y UL 2900-2-1 Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems.

[20] IEEE 2621 (partes 2621.1, 2621.2 y 2621.3) Normas para la seguridad de los dispositivos conectados para el tratamiento de la diabetes.

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

[22] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial.

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

8. ABREVIATURAS

AEMPS	Agencia Española de Medicamentos y Productos Sanitarios.
CC	Criterios Comunes / Common Criteria.
CCN	Centro Criptológico Nacional.
CE	Conformidad Europea (marcado CE).
COM-INI	Comunicación de Inicio de Expediente de inclusión.
CPSMED	Catálogo de Productos y Servicios Médicos Conectados.
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación.
DS	Declaración de Seguridad / Security Target.
EAL	Evaluation Assurance Level / Nivel de garantía de evaluación.
ENECSTI	Esquema Nacional de Evaluación y Certificación de la Seguridad de las TIC.
ENS	Esquema Nacional de Seguridad.
FOR	Formulario.
FSCA	Field Safety Corrective Action / Acción correctiva de seguridad en campo.
IA	Inteligencia Artificial.
IAD	Informe de Análisis Diferencial.
IEC	International Electrotechnical Commission.
IEEE	Institute of Electrical and Electronics Engineers.
IoMT	Internet of Medical Things / Internet de las cosas médicas.
ITE	Informe Técnico de Evaluación.
ITI	Informe Técnico de Inclusión.
IVDR	In Vitro Diagnostic Medical Devices Regulation (Reglamento (UE) 2017/746).
JR	Justificación de Requisitos.
LINCE	Certificación Nacional Esencial de Seguridad.
MDCG	Medical Device Coordination Group.
MDR	Medical Devices Regulation (Reglamento (UE) 2017/745).
MDS2	Manufacturer Disclosure Statement for Medical Device Security.
PES	Procedimiento de Empleo Seguro.
RFS	Requisitos Fundamentales de Seguridad.
RITI	Resultado del Informe Técnico de Inclusión.
RRPDS	Resultado de la Revisión de la Propuesta de Declaración de Seguridad.
SBOM	Software Bill of Materials / Lista de componentes software.
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.
UL	Underwriters Laboratories.