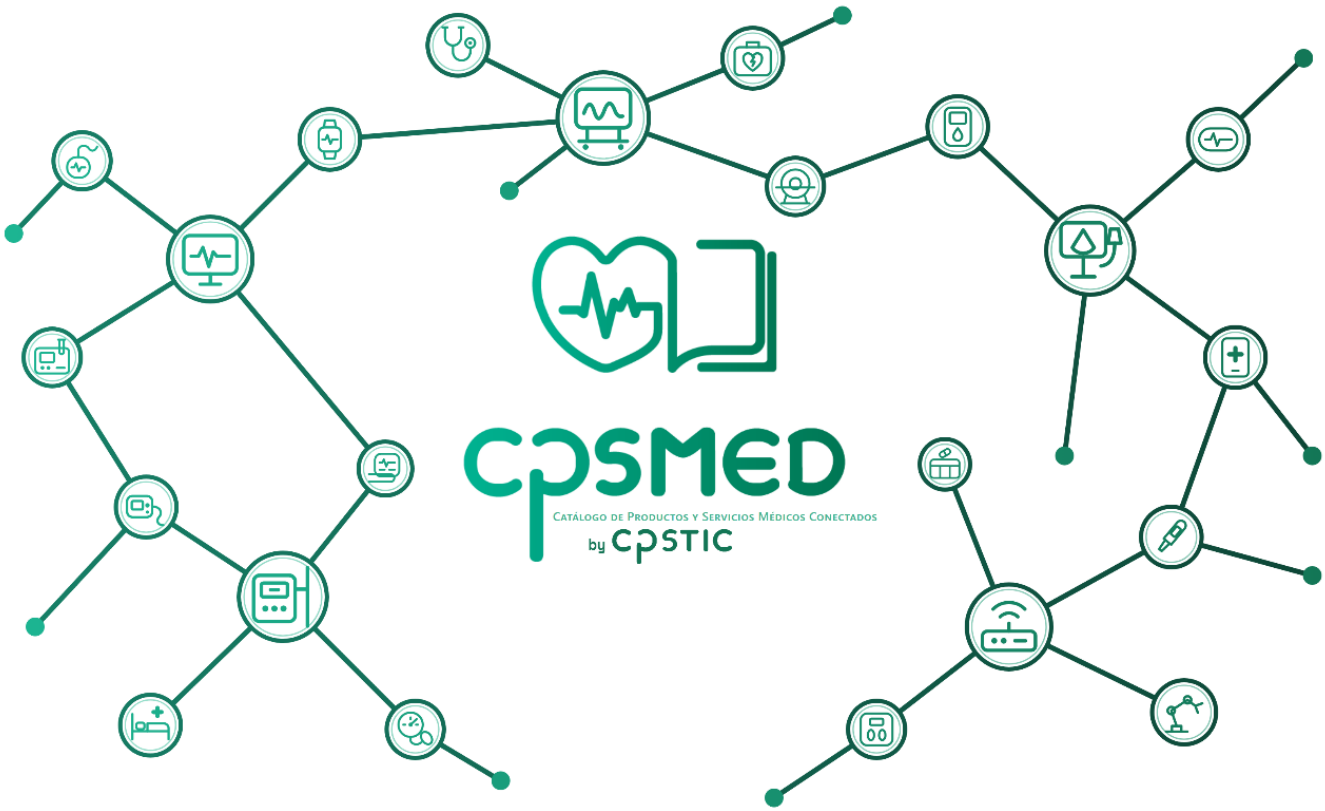
Guía de Seguridad de las TIC
CCN-STIC 163

Plantilla de Justificación de Requisitos (JR)



Noviembre 2026

Edita:

centro criptológico nacional

Versión: 1.0
Fecha de Edición: Noviembre de 2026

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

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 3
1.1 INFORMACIÓN DEL SOLICITANTE, DEL TOE Y DE LA EVALUACIÓN 3
1.2 APLICABILIDAD DE LOS REQUISITOS 4
2 JUSTIFICACIÓN DE LOS REQUISITOS 6
2.1 FS. NOMBRE DE LA FUNCIÓN DE SEGURIDAD 6
3 REFERENCIAS 8

1 INTRODUCCIÓN

Este documento es una plantilla de referencia para redactar la Justificación de Requisitos (JR), en la que el solicitante analiza la aplicabilidad de cada uno de los Requisitos Fundamentales de Seguridad (RFS) de la familia o familias de la taxonomía CCN-STIC-142 [1] a las que pertenece el producto sanitario conectado y su correspondencia con la Declaración de Seguridad (DS) o con la certificación aportada.

De acuerdo con el apartado 4.5.1.1 de la CCN-STIC-163 [2], la JR se aportará junto con la solicitud de inclusión en el CPSMED en los siguientes casos: a) productos con certificación en vigor, cuando existan diferencias entre los RFS de 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 (por ejemplo, una certificación UL 2900-2-1 en una familia cuyo anexo no la contemple), y b) productos sin certificación en vigor. Para las familias cuyo anexo no se haya publicado, la JR analizará los requisitos que el CCN haya comunicado por escrito al solicitante (apartado 3.2 de la CCN-STIC-163).

El CCN analizará la JR junto con la DS o, en su caso, con el alcance de la certificación: en la fase de revisión de la propuesta de declaración de seguridad (apartado 4.5.3 de la CCN-STIC-163 [2]), cuyo resultado se comunica mediante el Resultado de la Revisión de la Propuesta de Declaración de Seguridad (RRPDS), o, para los productos con certificación en vigor, en la fase de revisión de la certificación (apartado 4.5.4).

Dado que la inclusión en el CPSMED responde a un criterio de todo o nada, todos los RFS de la familia deberán quedar cubiertos por la DS, por la certificación aportada, por una Evaluación STIC Complementaria o por el entorno, con la justificación correspondiente. La calificación de un requisito como NO APLICABLE deberá justificarse de forma rigurosa en relación con la funcionalidad del producto y con el caso de uso del anexo de la familia.

Los textos en gris y cursiva son instrucciones para cumplimentar la plantilla y deberán eliminarse en la versión final del documento. Los textos entre corchetes y en cursiva deberán sustituirse por la información correspondiente.

1.1 INFORMACIÓN DEL SOLICITANTE, DEL TOE Y DE LA EVALUACIÓN

Nombre del solicitante	
Nombre del TOE	
Versión del TOE	
Tipo de evaluación	*[LINCE / Common Criteria / UL 2900-2-1 / Certificación específica de la familia (p. ej. IEEE 2621) / Evaluación STIC Complementaria]*

Certificación o evaluación de partida	*[Identificador del certificado o de la evaluación; si aún no existe, la certificación que se pretende obtener]*
Referencia y versión de la DS o del informe de certificación	*[Identificador, versión y fecha de la DS]*
Familia(s) de la taxonomía (CCN-STIC-142) y anexo de RFS	*[Familia o familias y anexo correspondiente; p. ej. Dispositivos de insulina – Anexo A.1. Si la familia no tiene anexo publicado, referencia y fecha de la comunicación del CCN con los requisitos aplicables]*
Criticidad de la familia	*[ALTA / MEDIA / BÁSICA, según la CCN-STIC-142]*
Finalidad prevista (MDR / IVDR)	*[Finalidad prevista declarada por el fabricante]*
Marcado CE	*[Declaración UE de conformidad o certificado del organismo notificado]*
Inteligencia artificial integrada	*[Sí / No. En caso afirmativo, componentes de IA, función y versión]*
Componentes desplegados en la nube	*[Sí / No. En caso afirmativo, componentes (p. ej., aplicación o servicio de gestión remota) y función]*
Caso de uso del anexo de la familia	*[p. ej. Caso de uso 1 – entorno hospitalario / Caso de uso 2 – movilidad clínica]*

1.2 APLICABILIDAD DE LOS REQUISITOS

Para cada RFS se debe analizar su aplicabilidad e indicar uno de los siguientes resultados:

- **COMPROBACIÓN DIRECTA (CD):** para aquellos requisitos que son aplicables y pueden ser evaluados por el laboratorio. Se incluyen en la Declaración de Seguridad (DS).

- **COMPROBACIÓN INDIRECTA (CI):** para aquellos requisitos que el laboratorio no puede probar y para los que el solicitante debe aportar la evidencia adecuada que los cubra. Se incluyen en la DS si la metodología lo contempla; en LINCE quedan fuera de la DS y las evidencias se aportan mediante una Evaluación STIC Complementaria. Si el requisito está cubierto por una certificación UL 2900-2-1 o por una certificación específica de la familia, se indicará el requisito o apartado de la norma que lo cubre, conforme a la tabla de trazabilidad del anexo de la familia o, en su defecto, a la equivalencia justificada en esta JR.
- **NO APLICABLE (NA):** para aquellos requisitos que no son aplicables (por ejemplo, requisitos específicos de hardware cuando el TOE es una solución software). No se incluyen en la DS y se proporciona una justificación de su no aplicabilidad.
- **INTEGRACIÓN (INT):** para aquellos requisitos cubiertos por un componente de integración definido en el entorno y configurado por el propio desarrollador o fabricante. Se incluyen en la DS, adaptando su redacción cuando sea necesario.
- **CUBIERTO (CU):** para aquellos requisitos cubiertos por un componente de integración definido en el entorno de ejecución y configurado por el usuario final o por la organización sanitaria, o cubiertos por un componente definido en el entorno de ejecución. En la DS se incluirá la redacción del requisito que realiza la llamada al componente que lo cubre.

2 JUSTIFICACIÓN DE LOS REQUISITOS

A continuación, se analiza la aplicabilidad de los RFS de la familia *[indicar familia]* para el producto *[indicar nombre del TOE]*.

Si una parte de un requisito puede comprobarse de forma directa y otra parte está cubierta mediante comprobación indirecta, integración o una evaluación o certificación previa, el requisito se dividirá en dos con el siguiente formato: REQ.XA (parte del requisito comprobada con CD) y REQ.XB (parte del requisito cubierta con CI, INT o CU). Si la parte B es CU, en la DS se incluirá la redacción del requisito que realiza la llamada al componente que lo cubre.

Se deberá analizar cada requisito de seguridad desde el punto de vista de cada uno de los actores para poder determinar su aplicabilidad. En el caso de que un requisito recaiga en más de un actor, se dividirá en tantos requisitos como actores se identifiquen, con el formato "REQ.X_actor" (por ejemplo, REQ.1_USER y REQ.1_VENDOR). Para ello se definen los siguientes actores:

a) Usuario final (USER): profesional sanitario, paciente o cuidador que utiliza el producto.

b) Fabricante del producto (VENDOR).

c) Organización sanitaria (HDO): centro o servicio sanitario responsable del despliegue del producto, de su integración en la red clínica y de su operación.

Se deberá indicar la aplicabilidad de cada uno de los requisitos en la tabla de la sección de cada función de seguridad, con el formato que se muestra a continuación.

2.1 FS. NOMBRE DE LA FUNCIÓN DE SEGURIDAD

En el título de esta sección se indicará el nombre de la función de seguridad *correspondiente. Deberán existir tantas secciones como funciones de seguridad. La columna «Justificación» explicará el resultado asignado y, en los requisitos CI, la evidencia aportada; será obligatoria para los requisitos NA, CI, INT y CU. La columna «RFS en DS» contendrá la redacción final del requisito tal y como se incluirá en la DS propuesta; se indicará «No aplica» en los requisitos NA y en los requisitos CI que, según la metodología, queden fuera de la DS. Las filas de ejemplo deberán eliminarse.*

RFS	Descripción	Actor	Aplicabilidad	Justificación	RFS en DS
IAU.1	*[Ejemplo] El TOE identifica y autentica a cada usuario administrador antes de otorgar acceso a las*	*VENDOR*	*CD*	*Funcionalidad implementada en el TOE y verificable por el laboratorio mediante pruebas funcionales.*	*[Redacción final del requisito en la DS, con las asignaciones completadas]*

	interfaces de gestión.				
AUD.4B	*[Ejemplo] Transmisión de la información de auditoría generada a una entidad externa utilizando un canal seguro.*	*HDO*	*CU*	*El TOE exporta los eventos al servidor de auditoría de la organización sanitaria mediante el canal seguro definido en COM.1; la organización sanitaria configura dicho servidor en la red clínica.*	*El TOE transmitirá la información de auditoría generada al servidor de auditoría definido en el entorno de ejecución utilizando un canal seguro (COM.1).*
CMD.1	*[Ejemplo] Comprobación de que la función médica se ejecuta sobre un dispositivo móvil de consumo que cumple las condiciones de seguridad exigidas.*	***VENDOR***	***NA***	***El producto no dispone de aplicaciones para dispositivos móviles de consumo; toda la interacción se realiza a través de la interfaz local del dispositivo, según la arquitectura descrita en la DS.***	*No aplica*

3 REFERENCIAS

En esta sección se deberán referenciar todos aquellos documentos que hayan sido empleados para el análisis de la justificación de los diferentes requisitos.

Referencia	Título, versión y fecha
[1]	CCN-STIC-142 Taxonomía de referencia para productos y servicios médicos conectados (IoMT) y anexo de RFS de la familia [indicar anexo].
[2]	Guía CCN-STIC-163 y sus anexos.
[3]	*[Declaración de Seguridad del producto: identificador, versión y fecha]*
[4]	*[Certificado e informe de certificación aportados: identificador, versión y fecha]*
[5]	*[Documentación regulatoria del producto sanitario: declaración UE de conformidad, instrucciones de uso]*