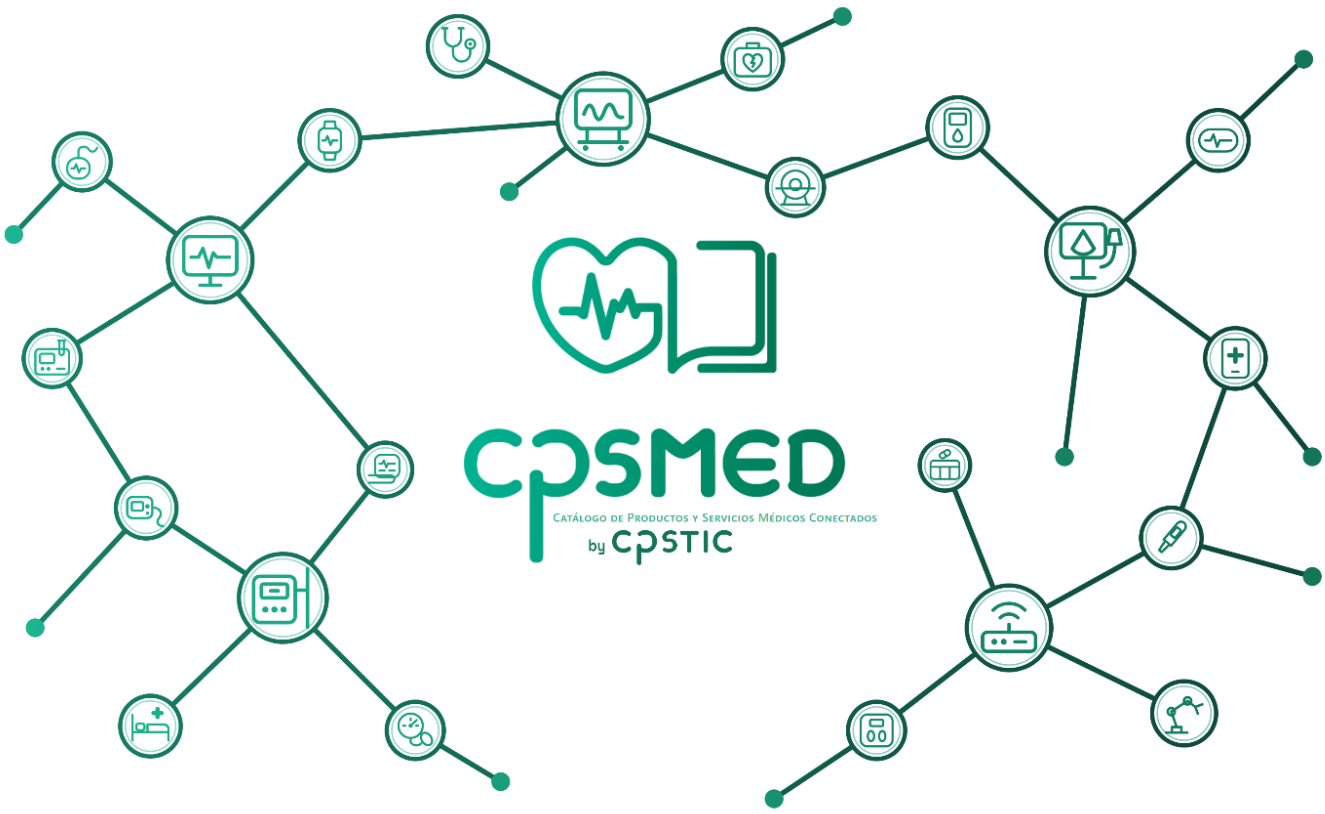
Guía de Seguridad de las TIC
CCN-STIC 142

Taxonomía de productos STIC -
Anexo A.1: Dispositivos de Insulina



Noviembre de 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 08:25:20 +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 Y OBJETO 3
2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS 4
2.1 FUNCIONALIDAD 4
2.2 CASOS DE USO 5
2.2.1. CASO DE USO 1 – EMPLEO DE LOS DISPOSITIVOS DE INSULINA EN UN ENTORNO HOSPITALARIO 5
2.2.2. CASO DE USO 2 – EMPLEO DE LOS DISPOSITIVOS DE INSULINA EN UN ENTORNO DE MOVILIDAD CLÍNICA 6
2.3 DELIMITACIÓN DEL ALCANCE DEL PRODUCTO 7
3. INCLUSIÓN EN EL CPSMED 8
4. PROBLEMA DE SEGURIDAD 9
4.1 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN 9
4.2 ACTIVOS SENSIBLES A PROTEGER 10
4.3 AMENAZAS 11
4.4 TRAZABILIDAD AMENAZAS Y FUNCIONES DE SEGURIDAD 13
5. REQUISITOS FUNDAMENTALES DE SEGURIDAD 14
5.1 ADMINISTRACIÓN 14
5.2 IDENTIFICACIÓN Y AUTENTICACIÓN 15
5.3 CANALES SEGUROS 18
5.4 CRIPTOGRAFÍA 19
5.5 INSTALACIÓN Y ACTUALIZACIÓN 20
5.6 AUDITORÍA 21
5.7 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES 24
5.8 PROTECCIÓN DEL PRODUCTO 25
5.9 CAPACIDADES ANTI-EXPLOTACIÓN 25
5.10 FUNCIONAMIENTO AUTÓNOMO 26
5.11 VERIFICACIÓN DE LA INTEGRIDAD DEL PRODUCTO Y DEL DATO 27
5.12 FLUJO DE DATOS 28
5.13 AUTORIZACIÓN DE CONEXIONES DE RED 29
5.14 DISPONIBILIDAD DE LA FUNCIÓN CLÍNICA 30
5.15 DISPOSITIVOS MÓVILES CONECTADOS A LOS DISPOSITIVOS MÉDICOS 33
6. ANEXO I: TRAZABILIDAD REQUISITOS DE SEGURIDAD PARA LINCE 35
7. ANEXO II: TRAZABILIDAD CON IEEE 2621 36
8. ABREVIATURAS 39

1. INTRODUCCIÓN Y OBJETO

El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia **Dispositivos de Insulina** para ser incluido en el Catálogo de Productos y Servicios Médicos Conectados (CPSMED), publicado por el CCN.

Estos requisitos representan las capacidades de seguridad mínimas que cualquier producto dentro de esta familia debe implementar para un determinado caso de uso, independientemente del fabricante y la tecnología, con el fin de proporcionar un nivel mínimo de confianza y considerarse objetivamente cualificado para ser empleado en los centros sanitarios para los que sea de aplicación el **Esquema Nacional de Seguridad (ENS).** Estos requisitos aportan mecanismos enfocados a reducir vulnerabilidades y contrarrestar amenazas, fundamentalmente de carácter técnico, aunque también pueden ser de naturaleza física o procedimental.

Además, la aplicación de estos criterios permitirá:

- Que se establezcan unas características mínimas de seguridad que sirvan de referencia a los **fabricantes** a la hora de desarrollar nuevos dispositivos médicos.
- Que los **organismos responsables de la adquisición** dispongan de evaluaciones completas, consistentes y técnicamente adecuadas, que permitan contrastar la eficacia y proporcionar información no sesgada acerca de los servicios de seguridad que ofrecen dichos productos.
- Que los **usuarios finales** posean una guía que facilite el despliegue y garantice el uso apropiado del producto desde el punto de vista de la seguridad.

Por lo tanto, los productos catalogados dentro de la familia **Dispositivos de Insulina** conforme a la taxonomía definida por el Centro Criptológico Nacional, serán susceptibles de ser evaluados usando como referencia este documento.

En el caso de productos multipropósito, queda fuera del alcance de este documento cualquier otra funcionalidad de seguridad proporcionada, más allá de la especificada para esta familia en la siguiente sección. Dichos productos podrían optar a ser incluidos de manera adicional en otra(s) familia(s) del CPSMED si cumpliesen los RFS correspondientes.

2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS

2.1 FUNCIONALIDAD

Los **Dispositivos de Insulina,** conocidos también como "connected diabetes devices" (CDD), son dispositivos médicos digitales destinados a la monitorización y al manejo de la diabetes. Estos dispositivos están compuestos por una plataforma hardware y un software de sistema. Todos estos dispositivos se caracterizan por intercambiar información a través de medios inalámbricos o cableados con otros CDD, con smartphones y/o con servidores en la nube, lo cual permite al paciente, a los cuidadores y a los profesionales sanitarios seguir y gestionar la terapia con mayor facilidad.

Esta familia de productos abarca el ecosistema completo de la terapia insulínica, es decir: los equipos de medición de glucosa, los de administración de insulina y los de control de terapia.

La funcionalidad común a este conjunto de dispositivos es que todos ellos adquieren o procesan los datos clínicos, almacenan dichos datos clínicos en la memoria local, los presentan al usuario y los transmiten o los reciben a través de canales de comunicación establecidos con otros dispositivos autorizados.

Atendiendo a la funcionalidad propia de cada uno, estos dispositivos se dividen en:

- **Medidor de glucosa en sangre (BGM-Blood Glucose Meter):** Determina de forma puntual el nivel de glucosa a partir de una muestra de sangre capilar depositada sobre una tira reactiva. El dispositivo analiza la muestra, calcula el valor de la glucosa (BG), lo muestra en pantalla y lo almacena en una memoria no volátil. Según el tipo de modelo, puede transferir las lecturas a un PC por USB o transmitirlas de forma inalámbrica a un receptor, como una bomba de insulina o un smartphone.
- **Monitor continuo de glucosa (CGM-Continuous Glucose Monitor):** Proporciona una medición continua de la glucosa a partir de un sensor que analiza el fluido intersticial, habitualmente adherido al cuerpo. El sensor transmite de forma inalámbrica sus lecturas al monitor o receptor, que las procesa, muestra tendencias y genera alerta ante hipo o hiperglucemias. Frente al BGM, este aporta seguimiento en tiempo real y datos de tendencia en lugar de valores aislados.
- **Bomba de Insulina (Insulin Pump):** Administra insulina por vía subcutánea de forma controlada, combinando la infusión basal continua con bolos puntuales. Puede funcionar de manera autónoma según su programación o recibir información de otros dispositivos (lecturas de glucosa de un BGM o comandos operativos desde un mando remoto). Además, se trata de un dispositivo de administración y, por tanto, crítico para la seguridad.
- **Sistema de dosificación automática de insulina (AID-Automated Insulin Dosing):** Es un sistema de lazo cerrado (aproximación al "páncreas artificial") que integra la entrada de glucosa de un CGM, la capacidad de administración de una bomba de insulina y un algoritmo de control que ajusta automáticamente la dosis en función de las lecturas de glucosa. En términos de evaluación, un AID puede ser un único dispositivo de un solo fabricante o estar compuesto por

varios CDD evaluados de forma independiente, incluso de fabricantes distintos, que operan de manera continua. Sin embargo, su principal función es automatizar la decisión terapéutica.

- **Mando o controlador remoto de insulina (Remote Controller):** Se trata de un dispositivo de mano o de una aplicación en un dispositivo de propósito general, cuya función es enviar comandos a otro CDD, típicamente a la bomba de insulina, a través de un canal inalámbrico (ordenar la administración de un bolo o modificar parámetros de la terapia). Sin embargo, este dispositivo no mide la glucosa ni administra la insulina por sí mismo, sino que actúa como una interfaz de control remota. Su importancia para la seguridad deriva de que un uso no autorizado de ese canal permitiría gobernar la administración de la insulina al paciente a distancia.
- **Otros dispositivos de insulina conectados:** la familia podrá abarcar otros CDD cuyos requisitos de seguridad resulten compatibles con los recogidos en este documento, como las plumas de insulina conectadas (Smart Insulin Pen), que registran las dosis administradas manualmente y las transmiten a una aplicación asociada. Aunque en estos dispositivos la administración es manual, la manipulación de los datos registrados podría inducir recomendaciones de dosis erróneas, por lo que les serán de aplicación los requisitos de este documento que correspondan a su funcionalidad, en particular los relativos a la integridad del dato y a los canales seguros.

2.2 CASOS DE USO

Dependiendo de las funcionalidades del producto explotadas y de la finalidad o el contexto en que se utilicen, se contemplan dos casos de uso para esta familia de productos, tal y como se definen a continuación.

2.2.1. CASO DE USO 1 – EMPLEO DE LOS DISPOSITIVOS DE INSULINA EN UN ENTORNO HOSPITALARIO

En este escenario, los dispositivos de insulina operan dentro del propio centro sanitario y son manejados por el personal clínico, no por el propio paciente. En consecuencia, el entorno físico está controlado, aunque los equipos son compartidos entre diferentes pacientes e integrados con el resto de sistemas del hospital. En este caso de uso, se suelen encontrar sobre todo BGM compartidos y CGM asignados a los pacientes, junto con bombas de insulina y AID bajo supervisión. Sin embargo, los mandos remotos de insulina apenas aparecen en esta casuística.

Además, una de las principales amenazas es su conexión con un equipo de la red interna del hospital que esté infectado por un malware.

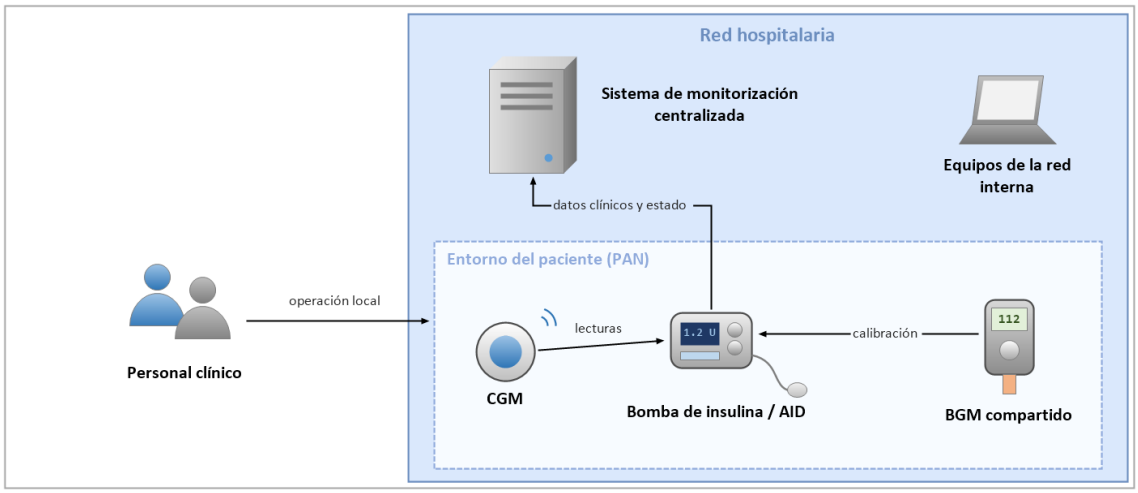


Figura 1 – Caso de Uso 1: Entorno Hospitalario

2.2.2. CASO DE USO 2 – EMPLEO DE LOS DISPOSITIVOS DE INSULINA EN UN ENTORNO DE MOVILIDAD CLÍNICA

En este escenario, los dispositivos de insulina acompañan al paciente en su vida diaria, además de poder ser manejados por el propio paciente o por un cuidador. En estos casos de uso pueden participar, de manera coordinada, distintas combinaciones de los dispositivos de insulina descritos anteriormente, sin que sea necesario el empleo de todos ellos; por ejemplo: el CGM que mide, la bomba de insulina que administra, el AID que cierra el lazo, el mando remoto de insulina que envía comandos o el BGM empleado para la calibración. También pueden emplearse plumas de insulina conectadas junto con un BGM o un CGM. Este entorno no está controlado, ni físicamente ni en la red.

Dado que el entorno no está controlado, ni físicamente ni en la red, una de las principales amenazas es la pérdida o robo del dispositivo, además del emparejamiento con un dispositivo de consumo infectado por un malware.

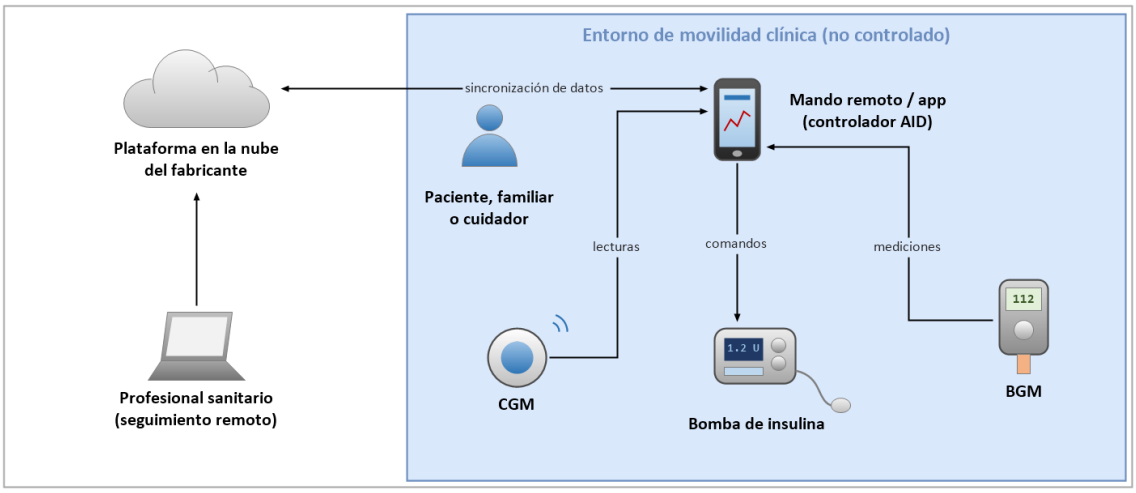


Figura 2 – Ejemplo de Caso de Uso: Movilidad Clínica

2.3 DELIMITACIÓN DEL ALCANCE DEL PRODUCTO

Los productos de esta familia pueden presentarse en distintos formatos según su naturaleza. En concreto, pueden presentarse como dispositivo dedicado (hardware provisto del firmware y software específicos para su función, como un medidor de glucosa, un monitor continuo de glucosa, una bomba de insulina o un mando remoto físico) o como aplicación software instalada sobre un dispositivo de propósito general (por ejemplo, un mando o controlador remoto implementado como aplicación en un teléfono inteligente).

En este último caso, la plataforma de propósito general sobre la que se ejecuta la aplicación no formará parte del alcance de la certificación, salvo la porción de dicha plataforma que intervenga directamente en el control o la ejecución de funciones críticas para la seguridad, que sí deberá incluirse bajo el alcance.

Quedan fuera del alcance de la evaluación los elementos que, aun cooperando con el dispositivo, no forman parte del TOE ni de sus funciones de seguridad.

En caso de que el correcto funcionamiento de la función principal del dispositivo requiera una aplicación software específica que se comunique con él (por ejemplo, una aplicación de control o de configuración imprescindible para su operación), dicha aplicación deberá incluirse bajo el alcance de la evaluación.

En el caso de los sistemas de dosificación automática de insulina (AID), el objeto de evaluación podrá estar constituido por un único dispositivo o por un conjunto de dispositivos que operan de forma coordinada, procedentes de uno o varios fabricantes. En este supuesto, cada dispositivo se evaluará de forma independiente frente a su propia declaración de seguridad, sin que la interacción entre ellos amplíe automáticamente la frontera de evaluación de ninguno de ellos.

Los escenarios no contemplados en este documento deberán ser analizados específicamente por el fabricante mediante un análisis de riesgos que justifique la aplicabilidad de los requisitos establecidos.

3. INCLUSIÓN EN EL CPSMED

Para que un producto de esta familia pueda ser incluido en el Catálogo de **CPSMED** deberá disponer de alguna de las siguientes certificaciones:

a) Certificación Nacional Esencial de Seguridad (LINCE).

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.

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.

d) Certificación IEEE 2621, 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*.

La certificación deberá incluir los RFS reflejados en el apartado 5, que deberán ser evaluados considerando el problema de seguridad definido en el presente documento.

En caso de que alguno de los requisitos indicados en el apartado 5 no se encuentre recogido en la declaración de seguridad del producto, pero este sí implemente esa función de seguridad, se podrá llevar a cabo una evaluación **STIC complementaria**, cuyo objetivo será verificar el cumplimiento de esos requisitos.

4. PROBLEMA DE SEGURIDAD

4.1 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN

Para la utilización en condiciones óptimas de seguridad de esta familia de productos, es necesario que se integre en un entorno de trabajo que cumpla una serie de condiciones mínimas de protección para ambos casos de uso:

- **Usuarios confiables bajo el control del usuario final**: Los usuarios con privilegios deben estar debidamente capacitados y carecer de cualquier intención maliciosa o conflicto de intereses dentro de su respectivo dominio de uso que puedan alterar o comprometer la integridad del producto. En el entorno hospitalario, este supuesto aplica al personal clínico que opera el dispositivo; en el entorno de movilidad clínica, al paciente o cuidador respecto de las funciones que tiene autorizado gestionar.

  Nota de aplicación: Un ***dominio de uso*** es el entorno delimitado dentro de un sistema o infraestructura que establece los límites de operación permitidos para los usuarios, definiendo qué recursos pueden gestionar, que acciones pueden ejecutar y en qué condiciones. Por lo tanto, cualquier acción fuera del dominio de uso establecido debe entenderse como potencialmente maliciosa.

  Nota de aplicación: Con intención de que el concepto *dominio de uso* aplicado en este documento no conduzca a error, se presentan los siguientes ejemplos:

  1) **Administrador de un dispositivo médico conectado que tiene una vulnerabilidad de desbordamiento de búfer.** Dentro de su dominio de uso, puede configurar los parámetros del dispositivo dentro de los rangos permitidos. Si explota la vulnerabilidad para ejecutar código arbitrario, saltarse los límites de seguridad o desactivar las alarmas, actúa de forma maliciosa. La vulnerabilidad supone una no conformidad del TOE, y los permisos de administración del usuario no la cubren.
  2) **Usuario autorizado de la aplicación de monitorización o de control del dispositivo, con una vulnerabilidad de ejecución remota de código (RCE).** Dentro de su dominio de uso, puede ver los datos, recibir las alertas y hacer las operaciones que le permite su perfil. Si explota la vulnerabilidad para ejecutar órdenes con privilegios elevados o enviar al dispositivo órdenes fuera de lo permitido, actúa fuera de su dominio de uso y de forma maliciosa. Esta vulnerabilidad también supone una no conformidad del TOE.

- **Protección física.** Cuando el producto se utilice en el entorno hospitalario (caso de uso 1), deberá estar protegido físicamente por su entorno operacional. No estará sujeto a ataques físicos que puedan comprometer su seguridad o interferir en su correcta operación. En caso de que el producto sea software, esta hipótesis aplica a la plataforma física sobre la que se ejecuta el producto.

  Nota de aplicación: Esta hipótesis no aplica al caso de uso 2 (movilidad clínica), en el que el dispositivo puede ser objeto de pérdida, robo o manipulación física. En ese escenario, la protección frente a accesos físicos no autorizados se cubre mediante los requisitos **PRO.1**, **PSC.1** y **PSC.3** (amenaza **A.NOAUT**).

- **Actualizaciones periódicas.** El *firmware/software* del producto es actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.

- **Protección de las credenciales.** Todas las credenciales, en especial la del administrador, deberán estar correctamente protegidas por parte de la organización que utilice el producto.

  Nota de aplicación: Esta hipótesis se considerará aplicable únicamente cuando el producto, o alguno de sus componentes (p. ej. la aplicación de control), se proporcione como un software a instalar sobre un dispositivo de propósito general, como un dispositivo móvil de consumo o un equipo del entorno hospitalario. En el caso de los dispositivos móviles de consumo, será de aplicación lo establecido en **CMD**.

- **Plataforma confiable.** El producto se ejecutará sobre una plataforma confiable, incluyendo el sistema operativo o cualquier entorno de ejecución que la plataforma proporcione.

  Nota de aplicación: Esta hipótesis se considerará aplicable únicamente cuando el producto, o alguno de sus componentes (p. ej. la aplicación de control), se proporcione como un software a instalar sobre un dispositivo de propósito general, como un dispositivo móvil de consumo o un equipo del entorno hospitalario. En el caso de los dispositivos móviles de consumo, será de aplicación lo establecido en **CMD**.

4.2 ACTIVOS SENSIBLES A PROTEGER

Los recursos que deben protegerse mediante el uso de esta familia de productos incluyen:

- **AC.PSS.** Datos de configuración, registros de auditoría y [***asignación**: listado de datos definidos por el fabricante]* que deben ser protegidos en Integridad.

- **AC.PSC**. Credenciales, claves privadas, datos del paciente y [**asignación**: *listado de datos definidos por el fabricante*] almacenados que deben ser protegidos en Confidencialidad e Integridad.

  Nota de aplicación: el activo "claves privadas" aplicará a las claves privadas usadas por el TOE para autenticarse en las comunicaciones.

- **AC.Comunicaciones.** Comunicaciones del producto, establecidas entre entidades autorizadas, que deben ser protegidas en Confidencialidad, Integridad y Autenticidad.

  Nota de aplicación: las entidades autorizadas hacen referencia a componentes del TOE, componentes del entorno operacional y usuarios (tanto administradores como no administradores) con acceso al TOE.

- **AC.Red**. Sistemas de la red en la que se integra el producto, dispositivos con los que mantiene una asociación y [**asignación:** *listado de sistemas definidos por el fabricante],* que deben ser protegidos en Integridad.

- **AC.FuncionClinica.** Función clínica del producto, recursos necesarios para ejecutarla (tiempo de cómputo, memoria, comunicaciones y alimentación) y [**asignación:** *listado de funciones clínicas definidas por el fabricante*], que deben ser protegidos en Integridad y Disponibilidad.

  Nota de aplicación: en esta familia, la función clínica comprende la adquisición de lecturas de glucosa, el cálculo y la administración de insulina y la gestión de alarmas clínicas.

4.3 AMENAZAS

Las principales amenazas a las que el uso de esta familia de productos pretende hacer frente son:

- **A.NOAUT Acceso a cambios en configuración no autorizado del producto**: Un atacante puede obtener acceso no autorizado al TOE, ya sea por la pérdida o robo del dispositivo, accediendo a través de interfaces de usuario normales (falta de autenticación de usuario) o mediante puertos de hardware físicos externos (ej. puertos JTAG o de programación Flash). Esto permite modificar configuraciones clave, alterar el firmware o extraer claves, comprometiendo la integridad del TOE y la seguridad clínica. Esta amenaza afecta a los activos *AC.PSS, AC.PSC y AC.FuncionClinica.*

- **A.MITM Ataques *Man In The Middle*:** Un atacante puede interceptar y modificar la comunicación entre dos entidades autorizadas comprometiendo la confidencialidad, integridad y autenticidad de los datos transmitidos. Esta amenaza afecta a los activos *AC.PSS, AC.PSC, AC.Comunicaciones y AC.FuncionClinica.*

- **A.ACT Actualización maliciosa**: Un atacante puede obtener un acceso no autorizado al TOE (cargar un firmware manipulado que contenga funciones ocultas) por medio de una actualización maliciosa que comprometa la integridad y autenticidad del producto. Esta amenaza afecta a los activos *AC.PSS*, *AC.PSC* y *AC.Comunicaciones*.
- **A.MEM Ataques de corrupción de memoria**: Un atacante puede explotar vulnerabilidades de gestión de memoria para inyectar y ejecutar código malicioso dentro del espacio de memoria del producto, comprometiendo la integridad del producto. Esta amenaza afecta a los activos *AC.PSS*, *AC.PSC* y *AC.Comunicaciones*.
- **A.MAL Malware y comportamiento anómalo:** El software cargado en el dispositivo o en su controlador móvil puede incluir código malicioso o explotable (incluido intencionalmente o por bibliotecas de terceros). Este software puede comprometer el correcto funcionamiento del TOE y otorgar privilegios adicionales a un atacante. Esta amenaza afecta a los activos *AC.PSS, AC.Red y AC.FuncionClinica.*
- **A.BAD_PEER Dispositivo Malicioso:** Un dispositivo de red que esté correctamente autenticado frente al TOE, pero que ha sido comprometido por un malware, puede llegar a actuar de manera maliciosa e intentar comprometer el dispositivo médico utilizando su conexión legítima previamente establecida. Esta amenaza afecta a los activos *AC.Comunicaciones, AC.PSS y AC.FuncionClinica.*
- **A.WEAK_CRYPTO Criptografía débil:** El uso de algoritmos insuficientes, longitudes de clave cortas, falta de entropía o implementaciones defectuosas pueden permitir a un atacante romper las protecciones de integridad y confidencialidad del dispositivo médico. Esta amenaza afecta a los activos *AC.PSC y AC.Comunicaciones.*
- **A.DOS Denegación del Servicio:** Un atacante puede provocar una denegación de servicio de manera intencionada, por ejemplo, mediante interferencias deliberadas (jamming) de las frecuencias de radio de red inalámbrica (PAN), mediante la saturación de los recursos computacionales (CPU, memoria) del TOE o mediante peticiones de conexión o de comunicación reiteradas que agoten su batería. Esta amenaza afecta a los activos *AC.Comunicaciones, AC.Red, AC.PSS y AC.FuncionClinica.*

4.4 TRAZABILIDAD AMENAZAS Y FUNCIONES DE SEGURIDAD

En la siguiente tabla se trazan qué funciones de seguridad definidas en el apartado 5 cubren las amenazas definidas en el apartado 4.3:

	A.NOAUT	A.MITM	A.ACT	A.MEM	A.MAL	A.BAD_PEER	A.WEAK_CRYPTO	A.DOS
ADM	X		X					
IAU	X							
CIF		X					X	
COM		X				X	X	
ACT			X		X			
AUD	X		X					
PSC	X							
PRO	X							
EXP				X	X			
FA								X
INT	X		X		X			
FLU					X	X		
ASO	X	X				X		
DIS					X	X		X
CMD					X	X		

5. REQUISITOS FUNDAMENTALES DE SEGURIDAD

A continuación, se recogen los requisitos fundamentales de seguridad que deben cumplir los productos que quieran optar a la inclusión en el CPSMED en esta familia.

En caso de que el producto no implemente la funcionalidad a la que aplica alguno de los requisitos (o algunas partes de ellos), y ésta sea proporcionada por el entorno operacional, el fabricante deberá indicarlo en la declaración de seguridad o justificarlo debidamente.

La convención utilizada en las descripciones de los RFS es la siguiente:

- Selección múltiple: se deberá seleccionar al menos una opción de las indicadas en el RFS y se incluirá en la declaración de seguridad. Ejemplo:

  RFS: Administración del producto [**selección múltiple***: local; remota*]

  DS: Administración del producto local y remota

- Selección única: se deberá seleccionar solo una opción de las indicadas en el RFS y se incluirá en la declaración de seguridad. Ejemplo:

  RFS: Administración del producto [**selección única***: local; remota*]

  DS: Administración del producto local

- Asignación: se deberá especificar el listado de opciones que sean de aplicación al TOE (podría no haber ninguna). Ejemplo:

  RFS: El TOE deberá identificar y autenticar a cada usuario administrador y [**asignación:** *otros usuarios del producto*] antes de otorgar acceso.

  DS: El TOE deberá identificar y autenticar a cada usuario administrador, auditor y usuario avanzado antes de otorgar acceso.

5.1 ADMINISTRACIÓN

Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional

ADM.1 El TOE debe definir el rol [**asignación:** *nombre del rol o roles de administrador*] como rol de administrador, y el rol [**asignación:** *nombre del rol o roles no administrativos*] como rol no administrativo para los usuarios de las interfaces de gestión. Además, el TOE debe ser capaz de asociar uno o más roles a estos usuarios.

ADM.2 El TOE debe permitir realizar de forma [**selección múltiple**: *local; remota*] las siguientes funcionalidades de gestión a través de las interfaces de gestión:

- Autorización y revocación de asociaciones permanentes con dispositivos remotos.
- Configuración de la política de control de flujo de información definida en **FLU.1.**
- Actualización del firmware/software del TOE.
- Consulta de los registros de auditoría generados por el TOE.

- [**asignación**: *otras funcionalidades administrables del producto*].

ADM.3 El TOE debe asegurar que solamente usuarios con permisos de administrador son capaces de realizar las funciones descritas en **ADM.2.**

Nota de aplicación: en el caso de que existan distintos tipos de administrador, cada uno de ellos con distintos permisos, deberá probarse que únicamente pueden realizar aquellas funcionalidades para las que tengan permiso.

Nota de aplicación: cuando la política de seguridad del TOE se defina durante su fabricación y no pueda modificarse posteriormente, el fabricante actuará como administrador, circunstancia que deberá declararse en la Declaración de Seguridad. En tal caso, las funcionalidades de **ADM.2** que no estén disponibles en el producto no se considerarán aplicables. Los accesos privilegiados de bajo nivel reservados al fabricante (por ejemplo, interfaces de fabricación o de servicio técnico) no se considerarán interfaces de gestión a efectos de **ADM.2** y **ADM.3**, si bien deberán declararse en la Declaración de Seguridad y su protección se valorará frente a la amenaza **A.NOAUT.**

En tal caso, solo podrán existir otros usuarios administradores (por ejemplo, el personal técnico del centro sanitario) con privilegios más restrictivos que los del fabricante, que no les permitan ampliar sus propios permisos ni modificar la política de seguridad definida en fabricación.

5.2 IDENTIFICACIÓN Y AUTENTICACIÓN

Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional

IAU.1 El TOE debe identificar y autenticar a cada usuario administrador y [**asignación:** *otros usuarios con roles no administrativos del producto*] antes de otorgar acceso a las interfaces de gestión, salvo para las siguientes funcionalidades: [**asignación:** *listado de funcionalidades*].

Nota de aplicación: las funcionalidades exceptuadas deberán limitarse a aquellas cuya indisponibilidad pueda comprometer la seguridad clínica del paciente, y su exclusión deberá justificarse en la Declaración de Seguridad.

IAU.2 El TOE debe implementar [**selección múltiple:** *bloqueo de usuarios durante [***asignación:** *tiempo de bloqueo*] tras [**asignación:** *número de intentos*] intentos fallidos; retardo creciente entre intentos consecutivos; 2FA; [**asignación:** *cualquier otro mecanismo de prevención de ataques por fuerza bruta validado por el CCN*]] para protegerse ante ataques de autenticación por fuerza bruta a las interfaces de gestión. El contador de intentos fallidos no debe reiniciarse al apagar y encender el TOE.

Nota de aplicación: La acción de respuesta seleccionada deberá justificarse ponderando la protección frente al acceso no autorizado y la disponibilidad de las funciones críticas para la seguridad del paciente. No se admitirá el bloqueo permanente cuando este impida al paciente acceder al tratamiento.

IAU.3 Cuando el TOE implemente mecanismos de autenticación basados en contraseñas o PIN, deberá aplicar como mínimo:

a) Longitud mínima:

   i. PIN numérico en la interfaz local del dispositivo: [**selección múltiple:** *bomba, controlador o mando*, [**asignación:** *otros dispositivos definidos por el usuario*]], de al menos [**asignación:** *número de dígitos igual o superior a 4*] dígitos.

   ii. Contraseña en las interfaces de gestión o remotas: [**selección múltiple:** *aplicación clínica; herramienta de configuración; consola del fabricante;* [**asignación**: *otras interfaces definidas por el usuario*]], de al menos [**asignación:** *número de caracteres igual o superior a 8*] caracteres.

b) Valores no permitidos: el TOE debe rechazar:

   i. PIN o contraseñas que sean secuencias (1234), repeticiones (0000) o (admin).

   ii. Valores que coincidan con el identificador o el número de serie del dispositivo.

   iii. Contraseñas incluidas en una lista de valores habituales o comprometidos.

   iv. [**asignación:** *otros criterios*].

c) Validez: no se exigirá la caducidad periódica. El TOE debe exigir el cambio [**selección múltiple***: tras un restablecimiento del dispositivo; cuando se sospeche que está comprometido; a petición del administrador*].

d) Renovación: para cambiar la contraseña o el PIN se debe [**selección única:** *autenticar al usuario con el valor vigente; contar con la autorización de un usuario con rol de administrador*], y el TOE debe impedir que se reutilice el valor inmediatamente anterior.

e) Protección:

   i. En el almacenamiento, no se guardarán en claro, sino mediante [**selección única:** *una función de derivación de claves o hash con sal autorizada por el CCN; un elemento seguro o zona de memoria del dispositivo protegida frente a su lectura externa*].

Nota de aplicación: en el caso de PIN numéricos, dado su reducido número de combinaciones posibles, el hash con sal no protege por sí solo frente a ataques de fuerza bruta fuera de línea, por lo que se recomienda su almacenamiento en un elemento seguro o zona de memoria protegida.

ii. En la transmisión, solo a través de un canal seguro conforme a **COM.1.**

iii. En la pantalla, se mostrarán enmascarados durante su introducción.

Nota de aplicación: este requisito no aplicará a mecanismos de autenticación alternativos que no utilicen contraseñas ni PIN.

IAU.4 El TOE debe [**selección única***: bloquear; cerrar*] la sesión de un usuario en la correspondiente interfaz de gestión después de [***asignación****: tiempo de inactividad inferior o igual a 30 minutos*] de inactividad.

Nota de aplicación: el tiempo máximo de inactividad debe ser de 30 minutos. Este requisito no será de aplicación a una interfaz de presentación continua de datos clínicos que requieran que el usuario mantenga la información visible, circunstancia que deberá justificarse en la Declaración de Seguridad.

IAU.5 Cuando el acceso se realice utilizando credenciales por defecto o el usuario no tenga asignadas credenciales a través de las interfaces de gestión, el TOE debe obligar al [**selección única***: cambio; establecimiento*] de credenciales en el siguiente acceso.

Nota de aplicación: este requisito será considerado aplicable únicamente a aquellos usuarios que sean creados desde el TOE una vez que se haya llevado a cabo el proceso de instalación y configuración segura del TOE.

IAU.6 El TOE debe autenticar al usuario mediante **[selección múltiple:** *PIN conforme a* ***IAU.3****;* **[asignación:** *otros mecanismos de autenticación*]] antes de emitir un comando con relevancia clínica desde **[selección múltiple:** *la aplicación del dispositivo móvil; el mando remoto;* **[asignación:** *otras interfaces*]], y debe volver a solicitar la autenticación tras **[asignación:** *tiempo máximo*] sin interacción del usuario. Este requisito no debe impedir la suspensión de la administración de insulina prevista en **DIS.7**.

5.3 CANALES SEGUROS

Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional

COM.1 El TOE debe establecer canales seguros cuando intercambie información sensible con entidades autorizadas: [**selección múltiple:** *servidor de auditoría;* [**asignación:** *otras entidades*]] o entre distintas partes del producto, usando [**selección múltiple:** *IPsec; SSHv2 o superior; TLS 1.2 o superior; DTLS 1.2 o superior; HTTPS sobre TLS 1.2 o superior; SFTP; HL7 sobre TLS 1.2 o superior; MQTT sobre TLS 1.2 o superior; Bluetooth LE con LE Secure Connections; IEEE 802.15.4 con seguridad de capa de enlace;* ***[asignación:*** *otros protocolos autorizados por el CCN]*] con los siguientes mecanismos criptográficos [**asignación:** *listado de mecanismos, cipher suites o curvas elípticas autorizadas por el CCN para cada protocolo en la CCN-STIC 807*].

Nota de aplicación: cuando se seleccione Bluetooth LE, no se admitirán los métodos de emparejamiento *Just Works* ni el modo *LE Legacy Pairing*, salvo que el canal se proteja adicionalmente a nivel de aplicación conforme a esta misma familia de requisitos.

COM.2 El TOE no debe iniciar ni permitir canales de comunicación adicionales a los definidos en **COM.1.**

COM.3 El TOE debe hacer uso de [**selección múltiple:** *certificados digitales, claves criptográficas pre-compartidas, Pairing keys protegidas por hardware*, [**asignación:** *otros mecanismos autorizados por el CCN en la CCN-STIC 807*]] para la autenticación mutua de los extremos del canal cuando utilice cualquiera de los protocolos definidos en **COM.1**.

Nota de aplicación: en los canales en los que el TOE actúe únicamente como cliente frente a un servidor (por ejemplo, el envío de datos a una plataforma en la nube), la autenticación del TOE ante el servidor podrá realizarse a nivel de aplicación (por ejemplo, mediante credenciales o tokens específicos del dispositivo) en lugar de mediante autenticación mutua en el propio protocolo, siempre que el TOE autentique al servidor y ambos extremos queden identificados de forma fiable.

COM.4 El TOE debe establecer canales seguros cuando intercambie información con los usuarios remotos, usando **[selección múltiple:** *IPsec; SSHv2 o superior; TLS 1.2 o superior; DTLS 1.2 o superior; HTTPS sobre TLS 1.2 o superior;* **[asignación:** *otros protocolos autorizados por el CCN*]] con los siguientes mecanismos criptográficos: **[asignación:** *listado de mecanismos, cipher suites o curvas elípticas autorizadas por el CCN para cada protocolo en la CCN-STIC 807*].

Nota de aplicación: este requisito será de aplicación únicamente cuando el TOE ofrezca interfaces de gestión o de consulta accesibles de forma remota por usuarios (por ejemplo, una consola web o en la nube del fabricante, o una aplicación clínica de seguimiento), y en particular cuando se seleccione la opción «remota» en **ADM.2.**

COM.5 El TOE debe detectar y rechazar la repetición de mensajes y comandos con relevancia clínica recibidos a través de los canales definidos en **COM.1**, mediante **[selección múltiple:** *números de secuencia o contadores monotónicos; valores de un solo uso (nonces); marcas temporales con ventana de validez limitada;* **[asignación:** *otros mecanismos*]].

Nota de aplicación: este requisito podrá considerarse satisfecho por el propio protocolo seleccionado en **COM.1** cuando este incorpore protección frente a la repetición (p. ej. TLS, DTLS o Bluetooth LE con LE Secure Connections y cifrado de enlace), siempre que el TOE no acepte comandos con relevancia clínica fuera de dicho canal.

COM.6 El TOE debe validar los certificados digitales que emplee para autenticar los extremos de los canales definidos en **COM.1** y **COM.4**, comprobando como mínimo la cadena de certificación hasta una autoridad de confianza, su periodo de validez y la correspondencia de su identidad con el extremo esperado, así como **[selección múltiple:** *su estado de revocación; la fijación (pinning) del certificado o de la clave pública del extremo;* **[asignación:** *otras comprobaciones*]*; ninguna otra*], y debe rechazar el establecimiento del canal cuando alguna de estas comprobaciones no resulte satisfactoria.

COM.7 El TOE no debe difundir en claro por sus interfaces inalámbricas datos clínicos ni **[selección múltiple:** *identificadores persistentes del dispositivo o del paciente;* **[asignación:** *otra información sensible*]], y debe emplear **[selección múltiple:** *direcciones privadas resolubles de Bluetooth LE; identificadores temporales que se renueven periódicamente;* **[asignación:** *otros mecanismos*]] cuando necesite anunciarse para establecer conexiones.

5.4 CRIPTOGRAFÍA

Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional

CIF.1 El TOE debe permitir exclusivamente el empleo de mecanismos criptográficos: [**asignación**: *listado de mecanismos en la CCN-STIC-807*] autorizados por el CCN.

CIF.2 El TOE debe generar y utilizar números aleatorios necesarios para **[selección múltiple:** *generación de claves; nonces de sesión; vectores de inicialización;* **[asignación:** *otros usos definidos por el fabricante*]] que cumplan con [**asignación:** *métrica de calidad o estándar criptográfico definido por el CCN*], asegurando que el generador es inicializado (*seeded*) con una entropía al menos igual a la mayor fortaleza de seguridad de las claves y hashes que será capaz de generar.

Nota de aplicación: este requisito se verificará cuando la generación de números aleatorios sea implementada por el propio TOE. Cuando dicha función se delegue en una biblioteca de terceros o en la plataforma subyacente, el fabricante deberá identificar el componente empleado y justificar su conformidad en la Declaración de Seguridad.

5.5 INSTALACIÓN Y ACTUALIZACIÓN

Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional

ACT.1 El TOE debe ofrecer la posibilidad de consultar la versión actual del firmware/software y poder [**selección única**: *actualizarse automáticamente; actualizarse manualmente; iniciar actualizaciones manualmente*] y [**selección única**: *comprobar si existen nuevas actualizaciones disponibles; ningún otro*].

ACT.2 El TOE debe utilizar mecanismos de firma digital autorizados por el CCN para autenticar las actualizaciones *firmware/software* antes de instalarlas.

ACT.3 El TOE debe permitir la actualización del *firmware/software* únicamente a usuarios con rol de administrador en la interfaz de gestión correspondiente.

ACT.4 El TOE debe estar empaquetado de forma que, si se elimina, no deje rastro de su instalación (excepto por configuraciones y ficheros de salida o auditoría).

Nota de aplicación: Este requisito se considerará aplicable únicamente cuando el producto se proporcione como software a instalar sobre un dispositivo de propósito general (por ejemplo, una aplicación de control o de monitorización en un teléfono inteligente, una tableta o un equipo del centro sanitario). No aplica cuando el producto sea un dispositivo médico con hardware y firmware propios.

ACT.5 El TOE no debe descargar, modificar, reemplazar o actualizar su propio código binario.

Nota de aplicación: Este requisito se considerará aplicable únicamente cuando el producto se proporcione como software a instalar sobre un dispositivo de propósito general (por ejemplo, una aplicación de control o de monitorización en un teléfono inteligente, una tableta o un equipo del centro sanitario). No aplica cuando el producto sea un dispositivo médico con hardware y firmware propios.

Además, este requisito no se considerará aplicable en el caso de que el TOE se actualice automáticamente, tal y como permite **ACT.1**.

ACT.6 El TOE debe rechazar la instalación de versiones de firmware/software anteriores a **[selección única:** *la versión instalada; una versión mínima de seguridad establecida por el fabricante y protegida en el TOE*], comprobando para ello **[selección múltiple:** *un contador de versión monotónico protegido frente a modificación; el número de versión incluido en el paquete firmado conforme a* ***ACT.2****;* **[asignación:** *otros mecanismos*]].

Nota de aplicación: el objetivo de este requisito es impedir que se instale una versión legítimamente firmada pero antigua, con vulnerabilidades conocidas, ya que la verificación de la firma exigida en **ACT.2** no lo evita por sí sola. La opción de versión mínima de seguridad permite revertir a versiones anteriores sin vulnerabilidades conocidas, por ejemplo ante un fallo funcional de la última versión.

5.6 AUDITORÍA

Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional

AUD.1 El TOE debe generar registros de auditoría cuando se produzca alguno de los siguientes eventos:

a) *Login* y *logout* de usuarios registrados en las interfaces de gestión.

b) Cambios en las credenciales de usuarios en las interfaces de gestión.

c) Cambios en la configuración del TOE tras llevar a cabo las acciones definidas en **ADM.2**.

d) Eventos relativos a la funcionalidad del producto:

i. **Encendido y apagado del TOE.** Debe registrarse la activación y desactivación del dispositivo (bomba, sensor o controlador).

ii. **Administración de insulina.** Debe registrarse el inicio, la finalización, la suspensión y la reanudación de la administración basal y de cada bolo, incluyendo tipo de administración, dosis

programada y administrada, y el origen de la orden (local, aplicación o algoritmo de lazo cerrado).

iii. **Cambios en la terapia.** Deben registrarse las modificaciones de los perfiles basales, ratios, factores de sensibilidad, objetivos glucémicos y límites de dosificación, indicando el valor anterior, el nuevo y el usuario o componente que los realiza.

iv. **Conexión y sustitución de consumibles y sensores.** Incluye el cambio de reservorio o cartucho, el cebado, la inserción o retirada de la cánula o del equipo de infusión y la inserción, el inicio, la calibración y la expiración del sensor de glucosa. Debe indicarse el tipo de elemento y su identificación si aplica.

v. **Generación, habilitación o deshabilitación de alarmas clínicas.** Debe registrarse el tipo de alarma (hipoglucemia, hiperglucemia, oclusión, reservorio bajo o vacío, fallo o pérdida de señal del sensor, batería baja, etc.).

vi. **Fallo de sensores o componentes internos del TOE.** Incluye fallos del motor o del mecanismo de dosificación, del sensor de oclusión, del sensor de glucosa, de la batería o de los módulos electrónicos. Debe indicarse el componente afectado y su identificador si aplica.

vii. **Pérdida de conexión con elementos externos.** Debe registrarse la pérdida o recuperación de conectividad entre la bomba, el sensor y el controlador o la aplicación móvil, así como con la plataforma clínica o del fabricante.

viii. **Actualizaciones de software y firmware.** Debe registrarse cada actualización aplicada al TOE, incluyendo tipo de actualización, identificador y versión.

ix. **Flujos de información denegados.** Debe registrarse la denegación de flujos por aplicación de la política definida en **FLU.1**, indicando fecha y hora, interfaz y operación afectada.

x. **Gestión de asociaciones.** Deben registrarse las asociaciones autorizadas y revocadas, así como las solicitudes de asociación rechazadas, indicando el identificador del dispositivo remoto y el resultado.

xi. **Rechazo de comandos con relevancia clínica.** Debe registrarse el rechazo de comandos por superar los límites de seguridad definidos en **FLU.5** o por detectarse su repetición conforme a **COM.5**, indicando el origen del comando y el motivo del rechazo.

xii. **Cambios de hora.** Debe registrarse cada modificación de la hora del sistema conforme a **AUD.6**, indicando la hora anterior, la nueva y el usuario o fuente que la realiza.

xiii. **Restablecimiento del dispositivo.** Debe registrarse la ejecución de la función definida en **PSC.2**. Cuando el restablecimiento elimine los registros, este evento deberá transmitirse antes a la entidad externa de **AUD.4.**

xiv. **Fallos de integridad y actualizaciones rechazadas.** Debe registrarse el resultado no satisfactorio de las verificaciones de **INT.4** y el rechazo de actualizaciones por no superar **ACT.2** o **ACT.6**, indicando el componente o la versión afectada.

xv. **Bloqueos por autenticación fallida.** Debe registrarse la activación del mecanismo definido en **IAU.2**, indicando la interfaz y el usuario.

xvi. [**asignación:** *listado de eventos*]**.**

AUD.2 Los registros de auditoría generados por el TOE deben contener, al menos, la siguiente información: *fecha y hora del evento, tipo de evento identificado, resultado del evento y usuario que produce el evento.*

Nota de aplicación: en caso de que el resultado de un evento presente más de un valor posible (típicamente, exitoso o fallido), **AUD.1** debe contemplar la generación de auditoría para todos los resultados posibles del evento.

AUD.3 El TOE debe aplicar la siguiente política de control de acceso a los registros de auditoría:

a) *Lectura:* usuarios autorizados.

b) *Modificación:* ningún usuario.

c) *Borrado:* [**selección única**: *solo administradores; ningún usuario*]

Nota de aplicación: en este requisito se deben declarar aquellos usuarios del TOE que puedan gestionar los registros de auditoría a través de las interfaces de gestión. En caso de que los registros de auditoría se puedan gestionar únicamente a través de ficheros del sistema operativo sobre el que se instale el TOE, se deberá indicar que ningún usuario puede leer, modificar o borrar dichos registros.

AUD.4 El TOE debe ser capaz de almacenar en sí mismo la información de auditoría generada y [**selección única**: *transmitir la información de auditoría*

*generada a una entidad externa utilizando un canal seguro **COM.1**; no transmitir la información de auditoría generada*].

AUD.5 El TOE deberá [**selección única**: *sobrescribir los registros siguiendo el criterio de mayor antigüedad; enviar a una entidad externa y eliminar; otra opción validada por el CCN*] en el caso de que el espacio para almacenamiento de los registros alcance su límite.

AUD.6 El TOE debe mantener una fuente de tiempo fiable para las marcas temporales de los registros de auditoría y para las funciones que dependan de la hora, obteniéndola de **[selección múltiple:** *un reloj interno de tiempo real; una fuente externa autenticada a través de un canal conforme a **COM.1**;* **[asignación:** *otras fuentes*]]. El TOE solo debe permitir la modificación de la hora a **[selección única:** *usuarios con rol de administrador; usuarios autorizados conforme a **IAU.1***] y debe registrar cada cambio de hora conforme a **AUD.1**.

Nota de aplicación: la hora del sistema condiciona tanto la validez de los registros de auditoría como la propia terapia, ya que un cambio malintencionado puede alterar la tasa basal aplicada en cada franja horaria o invalidar las marcas temporales empleadas conforme a **COM.5**. Los ajustes legítimos (p. ej. cambio de zona horaria o de horario estacional) deben realizarse sin pérdida de coherencia de los registros ya almacenados.

5.7 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional

PSC.1 El TOE debe almacenar las [**selección múltiple***: credenciales; claves privadas; clave anti-tamper; [**asignación**: otros parámetros de seguridad críticos definidos en el activo **AC.PSC***]] utilizando mecanismos criptográficos que cumplan con **CIF.1**.

Nota de aplicación: este requisito será de aplicación cuando el TOE almacene alguno de los parámetros indicados. Los datos del paciente incluidos en el activo **AC.PSC** deberán almacenarse protegidos conforme a este requisito y a **PSC.3**.

PSC.2 El TOE debe proporcionar a los usuarios con rol de administrador una función de restablecimiento que, antes de la reasignación del dispositivo a otro paciente o de su retirada del servicio, elimine de forma irrecuperable **[selección múltiple:** *los datos clínicos y de terapia del paciente; las asociaciones permanentes establecidas conforme a **ASO.1**; las credenciales y claves de los usuarios;* **[asignación:** *otros datos*]] y devuelva el TOE a una configuración inicial segura.

Nota de aplicación: este requisito aplica especialmente al caso de uso 1, en el que los dispositivos se reutilizan entre pacientes. No aplica a los componentes de un solo uso (p. ej. sensores de glucosa desechables). La eliminación podrá realizarse por sobrescritura o mediante borrado criptográfico, destruyendo las claves con las que se protegen los datos almacenados.

PSC.3 El TOE debe proteger la confidencialidad de **[selección múltiple:** *lecturas de glucosa; historial de administración de insulina; perfiles de terapia; datos identificativos del paciente;* **[asignación:** *otros datos almacenados en él*]] mediante **[selección múltiple:** *cifrado conforme a* ***CIF.1****; su almacenamiento en un elemento seguro o zona de memoria del dispositivo protegida frente a su lectura externa; ninguno, cuando el TOE no almacene datos identificativos del paciente y así se justifique en la Declaración de Seguridad*].

Nota de aplicación: este requisito es especialmente relevante en el caso de uso 2, en el que la pérdida o sustracción del dispositivo o del dispositivo móvil asociado es una amenaza principal. Cuando se seleccione el cifrado, el borrado criptográfico previsto en **PSC.2** podrá realizarse mediante la destrucción de las claves correspondientes.

PSC.4 El TOE debe garantizar que **[selección múltiple:** *las credenciales de acceso; las claves criptográficas;* **[asignación:** *otros parámetros de seguridad críticos*]] no se compartan entre distintos dispositivos, empleando para ello **[selección múltiple:** *la generación en el propio TOE durante su primera puesta en marcha; la inyección individualizada durante la fabricación;* **[asignación:** *otros mecanismos*]]. Además, el TOE no debe contener credenciales embebidas en el código, cuentas ocultas ni mecanismos de acceso no declarados en la Declaración de Seguridad.

5.8 PROTECCIÓN DEL PRODUCTO

Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional

PRO.1 El TOE debe resistir **[selección múltiple:** *el acceso a través de puertos de depuración o programación (p. ej. JTAG, SWD);* **[asignación:** *otros escenarios de manipulación física*]] mediante **[selección múltiple:** *su deshabilitación permanente en producción; su protección mediante autenticación;* **[asignación:** *otros mecanismos*]].

5.9 CAPACIDADES ANTI-EXPLOTACIÓN

Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional

EXP.1 Cuando el TOE se encuentre en ejecución, este no debe solicitar la asignación de ninguna dirección explícita de memoria del sistema, ni asignar memoria con permisos simultáneos de escritura y ejecución.

Nota de aplicación: en componentes basados en microcontroladores que carezcan de unidad de gestión o protección de memoria, el fabricante deberá justificar en la Declaración de Seguridad la no aplicabilidad de este requisito y describir las medidas equivalentes adoptadas.

EXP.2 El TOE debe estar configurado por defecto con permisos de ficheros que lo protejan de accesos no autorizados.

Nota de aplicación: este requisito se considerará aplicable cuando el TOE se ejecute sobre un sistema operativo con sistema de ficheros, como una aplicación en un teléfono inteligente o una tableta, o un controlador basado en Linux o Android embebido. No será de aplicación al firmware que carezca de sistema de ficheros.

EXP.3 El TOE debe estar compilado con protecciones contra *stack-based buffer overflow* habilitadas.

Nota de aplicación: este requisito aplica al firmware del dispositivo médico y a todo componente desarrollado en lenguajes sin gestión segura de memoria (por ejemplo, C o C++). Cuando el TOE sea una aplicación desarrollada en un lenguaje con gestión segura de memoria, aplicará únicamente a los componentes nativos que incluya.

5.10 FUNCIONAMIENTO AUTÓNOMO

Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional

FA.1.1 El TOE debe mantenerse operativo, sin depender de sistemas externos, en caso de pérdida de conectividad; indisponibilidad de los sistemas externos o **[asignación:** *otras causas definidas por el usuario, ninguna*], ejecutando las siguientes funciones: **[asignación:** *listado de funciones clínicas críticas*].

FA.1.2 El TOE debe suspender la administración de insulina, alertar al usuario y ofrecer la conmutación al modo manual previsto en **DIS.2** cuando dicha administración dependa de un dato que no haya sido recibido. Mientras persista la situación, el TOE debe **[selección múltiple:** *reintentar periódicamente la recepción de los datos; ejecutar un diagnóstico de las comunicaciones o del componente afectado;* **[asignación:** *otras acciones*]], y solo podrá reanudar la administración automática cuando vuelva a recibir datos válidos y actualizados.

FA.2 El TOE debe almacenar localmente las copias de seguridad, los parámetros de infusión, los datos clínicos asociados al paciente y los eventos generados durante los periodos de desconexión con los sistemas externos, asegurando su posterior sincronización mediante canales seguros cuando la conectividad sea restablecida.

5.11 VERIFICACIÓN DE LA INTEGRIDAD DEL PRODUCTO Y DEL DATO

Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional

INT.1 El TOE debe generar una evidencia que permita comprobar que el dato no ha sido modificado desde su registro para: lecturas de glucosa, parámetros de dosificación, datos de calibración que el TOE almacene y **[asignación:** *listado de objetos o tipos de información*].

INT.2 El TOE debe proporcionar a **[asignación:** *listado de sujetos*] la capacidad de comprobar la integridad de la información indicada en **INT.1**, a través de las evidencias generadas.

Nota de aplicación: los sujetos declarados pueden ser el propio TOE, el usuario a través de sus interfaces, o un dispositivo asociado que reciba los datos y necesite confirmar su validez antes de emplearlos, como una bomba de insulina que recibe lecturas de un monitor continuo de glucosa.

INT.3 La evidencia de validez exigida en **INT.1** debe consistir en **[selección única:** *una firma digital; un código de autenticación de mensaje*] calculado sobre el dato protegido mediante mecanismos autorizados por el CCN, verificado por firmware inmutable y apoyado en una raíz de confianza protegida por hardware y confiada por el fabricante.

Nota de aplicación: el objetivo de este requisito es que un atacante que consiga modificar el dato almacenado no pueda generar una evidencia válida para el dato manipulado. Por ello, no se considerará válido ningún mecanismo criptográfico que no esté aceptado por el CCN.

INT.4 El TOE debe verificar la integridad y autenticidad de la totalidad de su firmware y software durante el arranque y con anterioridad a su ejecución, así como **[selección múltiple:** *periódicamente durante la operación normal del producto; a petición de un usuario autorizado; ninguna*], mediante **[selección única:** *firma digital; código de autenticación de mensaje*] basado en mecanismos autorizados por el CCN, validado por firmware inmutable y anclado en una raíz de confianza protegida por hardware y confiada por el fabricante. Además, durante el arranque, el TOE debe verificar **[selección múltiple:** *el correcto funcionamiento de los mecanismos criptográficos;* **[asignación:** *otros*]; *ninguno*].

INT.5 Cuando la verificación exigida en **INT.4** no resulte satisfactoria, el TOE no debe ejecutar el componente afectado, debe advertir al usuario y debe ejecutar las siguientes acciones: **[asignación:** *listado de acciones*].

5.12 FLUJO DE DATOS

Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional

FLU.1 El TOE debe aplicar una política de control de flujo de información de red sobre los siguientes sujetos: **[selección múltiple:** *interfaces de red del TOE; dispositivos asociados;* **[asignación:** *otros sujetos*]]; información: **[selección múltiple:** *lecturas de glucosa; comandos de dosificación; datos de configuración; registros de auditoría;* **[asignación:** *otra información*]]; y operaciones: **[selección múltiple:** *envío; recepción;* **[asignación:** *otras operaciones*]].

FLU.2 El TOE solo debe permitir los flujos de información definidos en **FLU.1** cuando se cumplan las siguientes reglas: el dispositivo remoto está asociado conforme a **ASO.1** y autenticado conforme a **COM.3**; el tipo de información y la operación están autorizados para ese dispositivo remoto; y los comandos de dosificación proceden únicamente de dispositivos remotos autorizados para emitirlos. Además, el TOE debe aplicar las siguientes reglas: [**asignación:** *otras reglas de control de flujo, o ninguna*].

FLU.3 El TOE debe denegar por defecto todo flujo de información no permitido expresamente conforme a **FLU.2**, aunque el dispositivo remoto haya sido autenticado conforme a **COM.1** o asociado conforme a **ASO.1**.

FLU.4 El TOE debe descartar, antes de procesarlos, los datos recibidos a través de cualquier conexión establecida que no se ajusten al formato, la longitud y el rango de valores declarados para cada operación.

FLU.5 El TOE debe rechazar cualquier comando de administración de insulina que supere los siguientes límites de seguridad: **[selección múltiple:** *dosis máxima por bolo; tasa basal máxima; dosis total máxima en un periodo de* **[asignación:** *periodo*]; **[asignación:** *otros límites*]], con independencia de su origen (interfaz local, aplicación o algoritmo de lazo cerrado). Estos límites solo podrán ser modificados por un usuario con rol de administrador a través de **[selección única:** *la interfaz local del TOE; la interfaz local del TOE o una interfaz remota protegida conforme a* ***COM.1*** *y* ***COM.3***].

Nota de aplicación: el rechazo de un comando por superar los límites debe notificarse al usuario y registrarse conforme a **AUD.1**. Se recomienda seleccionar la modificación exclusivamente local, de modo que el compromiso de la aplicación o del canal remoto no permita alterar los límites de seguridad.

5.13 AUTORIZACIÓN DE CONEXIONES DE RED

Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional

ASO.1 El TOE debe requerir la autorización explícita del usuario para el establecimiento de una asociación de conexión permanente con un dispositivo remoto. Dicha autorización debe realizarse mediante una interacción directa del usuario con el TOE: **[selección múltiple:** *pulsación de un control físico del TOE; confirmación en la pantalla del TOE; introducción en el dispositivo remoto de un código generado y mostrado por el TOE;* **[asignación:** *otro mecanismo de interacción directa*]], de forma que ningún software pueda crear la asociación de forma programática.

Nota de aplicación: este requisito está previsto para las redes que ofrezcan autorización de usuario para las asociaciones de conexión. Cuando la tecnología de red empleada no la ofrezca, el fabricante debe declararlo y describir el mecanismo alternativo que impide la creación programática de asociaciones, cuya fortaleza deberá justificarse conforme a **ASO.2**.

ASO.2 El TOE debe verificar que el dispositivo remoto con el que establece la asociación autorizada conforme a **ASO.1** es el elegido por el usuario y no otro dispositivo que se encuentre dentro del alcance de la red inalámbrica. Para ello, debe autenticar a dicho dispositivo durante el proceso de asociación mediante [**selección múltiple:** *un código de emparejamiento de al menos* [**asignación:** *número*] *dígitos, generado aleatoriamente por el TOE en cada asociación, que el usuario debe introducir en el dispositivo remoto; un intercambio de claves autenticado fuera de banda;* [**asignación:** *otro mecanismo autorizado por el CCN*]]. En ningún caso dicha autenticación podrá basarse únicamente en identificadores accesibles sin interacción con el dispositivo, como los números de serie impresos en el producto, mostrados en su pantalla o difundidos por sus interfaces de red.

Nota de aplicación: **ASO.1** garantiza que la asociación solo se inicia por decisión del usuario, mientras que **ASO.2** garantiza que se establece con el dispositivo que el usuario pretende asociar, impidiendo que un atacante próximo lo suplante durante el proceso. Un mismo mecanismo puede satisfacer ambos requisitos: por ejemplo, la introducción manual por el usuario en el dispositivo remoto del código mostrado por el TOE acredita su autorización conforme a **ASO.1** y, a la vez, autentica al dispositivo remoto conforme a **ASO.2**.

Nota de aplicación: el acceso no autorizado a números de serie únicos impresos o mostrados podría emplearse para establecer conexiones remotas maliciosas, aunque autenticadas a nivel de dispositivo. Cuando se emplee el código de emparejamiento previsto en este requisito, dicho código debe ser de un solo uso y válido únicamente durante el periodo definido en **ASO.3**.

ASO.3 El TOE solo debe aceptar solicitudes de asociación durante un periodo limitado, que comenzará cuando el usuario realice la interacción prevista en **ASO.1** y que el TOE debe finalizar automáticamente transcurrido [**asignación:** *tiempo máximo*] o una vez completada la asociación. Fuera de dicho periodo, el TOE debe rechazar toda solicitud de asociación.

ASO.4 El TOE debe permitir a los usuarios autenticados conforme a **IAU.1** consultar las asociaciones permanentes activas, y únicamente a los usuarios con rol de administrador, conforme a **ADM.3**, revocar cualquiera de ellas, sin necesidad de acceder a interfaces de mantenimiento no documentadas. La revocación debe impedir de forma efectiva toda comunicación posterior con el dispositivo revocado hasta que se establezca una nueva asociación conforme a **ASO.1.**

ASO.5 El TOE debe limitar el número de asociaciones permanentes simultáneas a **[asignación:** *número máximo por tipo de dispositivo*], conforme a su funcionalidad declarada en la Declaración de Seguridad, y debe rechazar las solicitudes que excedan dicho límite.

5.14 DISPONIBILIDAD DE LA FUNCIÓN CLÍNICA

Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional

DIS.1 El TOE debe avisar al usuario cuando alguna de sus funciones críticas no se complete en el tiempo máximo previsto o cuando los recursos que necesita para ejecutarlas estén próximos a agotarse, con antelación suficiente para que el usuario pueda actuar:

- Funciones críticas: [**selección múltiple:** *adquisición de lecturas de glucosa; cálculo de la dosis de insulina; administración de insulina; gestión de alarmas*

clínicas; [**asignación:** *otras funciones críticas*]], con el siguiente tiempo máximo de ejecución para cada una: [**asignación:** *tiempo máximo por función*].

- Recursos vigilados: **[selección múltiple:** *capacidad de cómputo; memoria; comunicaciones; batería;* **[asignación:** *otros recursos*]], con el siguiente umbral de aviso para cada uno: **[asignación:** *umbral de aviso por recurso*].

Nota de aplicación: esta detección puede realizarla el propio TOE u otro de los dispositivos médicos de la solución, pero no debe depender únicamente del elemento cuyo fallo se quiere detectar.

DIS.2 El TOE debe abandonar de forma automática la ejecución autónoma de un tratamiento cuando detecte un fallo conforme a **DIS.1** o **DIS.3**, así como en los siguientes casos: [**asignación:** *otras condiciones de activación, o ninguna*], y debe permitir además que un usuario autenticado conforme a **IAU.1** lo haga desde la interfaz local del TOE. En ambos casos, el TOE debe avisar al usuario de la conmutación y proporcionarle un procedimiento para realizar el tratamiento de forma manual mediante [**selección múltiple:** *instrucciones mostradas en la interfaz del TOE; instrucciones mostradas en la aplicación asociada;* [**asignación:** *otros medios*]].

Nota de aplicación: este requisito no será de aplicación cuando el TOE no participe en la ejecución autónoma de un tratamiento, circunstancia que deberá declararse en la Declaración de Seguridad. Se entiende por operación autónoma aquella en la que el TOE calcula y administra el tratamiento sin intervención del usuario, a partir de datos recibidos de otros dispositivos.

DIS.3 El TOE debe avisar al usuario mediante **[selección múltiple:** *alerta sonora; alerta visual; vibración; notificación a los dispositivos asociados*] cuando detecte un fallo de comunicación con los dispositivos asociados que pueda poner en riesgo al paciente e indicarle las acciones que debe llevar a cabo.

Nota de aplicación: entre los fallos que deben considerarse se encuentran la inhibición deliberada de las frecuencias empleadas, el fallo de los componentes de radiofrecuencia, las amenazas de inmunidad radiada procedentes de entornos adyacentes y la interrupción de la comunicación con cualquiera de los extremos.

DIS.4 El TOE debe pasar a un modo de funcionamiento alternativo que no suponga un riesgo significativo para el paciente cuando falle la comunicación o un dispositivo asociado: [**asignación:** *descripción del modo alternativo o degradado*]. El TOE debe indicar claramente al usuario que está funcionando en ese modo y volver al funcionamiento normal cuando se restablezcan la comunicación o el dispositivo asociado, [**selección única***: de forma automática,*

una vez restablecido el canal seguro conforme a ***COM.1*** *y* ***COM.3****; previa confirmación del usuario en la interfaz local del TOE*].

Nota de aplicación: cuando el TOE participe en la ejecución autónoma de un tratamiento, el modo alternativo incluirá la conmutación prevista en **DIS.2.** En todos los casos, debe resultar evidente para el paciente que la solución opera de forma degradada.

DIS.5 El TOE debe seguir funcionando durante al menos **[asignación:** *tiempo*] en caso de que la red sufra una denegación de servicio, de forma que el usuario disponga de margen suficiente para detectar el problema y actuar antes de que suponga un riesgo para el paciente.

DIS.6 El TOE debe mantener su operación segura ante el fallo de cualquiera de los siguientes elementos de la solución, incluido su funcionamiento erróneo (por ejemplo, el envío de datos o comandos incorrectos): [**selección múltiple:** *la aplicación del dispositivo móvil; el mando remoto; el monitor continuo de glucosa; el controlador que ejecuta el algoritmo de lazo cerrado; el servicio en la nube;* [**asignación:** *otros elementos*]]. Para ello, debe aplicar los siguientes mecanismos: [**selección múltiple:** *límites de seguridad conforme a* ***FLU.5****; comprobación de la coherencia de los datos recibidos; confirmación por el usuario, en el propio TOE, de los comandos remotos;* [**asignación:** *otros mecanismos*]] y, cuando el elemento deje de estar disponible, pasar al modo alternativo previsto en **DIS.4**.

Nota de aplicación: el fallo del elemento que actúa como controlador inteligente resulta especialmente difícil de gestionar con seguridad, dado que tanto la operación médica como los propios mecanismos de detección de fallo pueden quedar comprometidos. Un ejemplo de redundancia recogido en la norma es la doble comprobación por el usuario, en el propio dispositivo médico dotado de pantalla, de un comando recibido de forma remota.

DIS.7 El TOE debe permitir en todo momento suspender la administración de insulina desde su interfaz local, sin depender de la disponibilidad de los dispositivos asociados ni de los canales de comunicación, y no debe permitir que un comando remoto **[selección única:** *reanude la administración suspendida localmente; reanude la administración o modifique la terapia mientras permanezca suspendida localmente*] sin la confirmación del usuario en la interfaz local del TOE. La suspensión local tendrá prioridad sobre cualquier acción remota.

Nota de aplicación: Ante la pérdida de conectividad o de funcionalidades no esenciales, el dispositivo deberá mantener, siempre que sea posible y conforme a su diseño previsto, las funciones necesarias para garantizar la continuidad segura de la terapia.

Nota de aplicación: este requisito aplica únicamente a los dispositivos que administran insulina (bomba de insulina o AID). La suspensión local no deberá quedar bloqueada por la autenticación del usuario: podrá declararse como excepción en **IAU.1**, de modo que pueda realizarse en una situación de emergencia o aunque el usuario esté bloqueado conforme a **IAU.2**. La reanudación, en cambio, sí deberá respetar la autenticación exigida en **IAU.1**.

DIS.8 El TOE no debe permitir que las alarmas clínicas **[selección múltiple:** *hipoglucemia; hiperglucemia; oclusión; reservorio bajo o vacío; fallo o pérdida de señal del sensor; batería baja;* **[asignación:** *otras alarmas*]] se desactiven, se silencien de forma permanente o vean modificados sus umbrales mediante comandos recibidos de forma remota, salvo **[selección única:** *ninguna excepción; su aplazamiento temporal durante* **[asignación:** *tiempo máximo*]*, que deberá indicarse en la interfaz local del TOE*].

Nota de aplicación: este requisito no limita la gestión de las alarmas por un usuario autorizado desde la interfaz local del TOE, cuyas modificaciones deberán registrarse conforme a **AUD.1**.

5.15 DISPOSITIVOS MÓVILES CONECTADOS A LOS DISPOSITIVOS MÉDICOS

Esta sección solo es de aplicación cuando la solución utilice un dispositivo móvil de consumo para manejar el dispositivo médico o para ejecutar parte del cálculo del tratamiento. Cuando no sea el caso, deberá declararse así en la Declaración de Seguridad.

CMD.1 El TOE debe comprobar que la función médica se ejecuta sobre un dispositivo móvil de consumo que cumple las siguientes condiciones: **[selección múltiple:** *arranque verificado anclado en hardware; recepción de actualizaciones de seguridad periódicas; presencia de controles frente a software malicioso, incluida la restricción de instalación de aplicaciones procedentes de fuentes o desarrolladores no confiables*].

Nota de aplicación: se considera que un dispositivo móvil certificado frente a la versión vigente de un perfil de protección de funcionalidad fundamental para dispositivos móviles satisface las tres condiciones. La comprobación debe realizarla tanto la aplicación alojada en el dispositivo móvil como el software del dispositivo médico asociado, cuando ambos formen parte del TOE.

CMD.2 El TOE debe realizar la comprobación exigida en **CMD.1** mediante **[selección múltiple:** *verificación frente a una lista de modelos permitidos; interfaces de atestación del sistema operativo; atestación remota respaldada por hardware*], y debe detectar si el dispositivo móvil ha sido rooteado o sometido a jailbreak. La comprobación debe efectuarse **[selección múltiple:** *al iniciar la aplicación; durante su uso*].

CMD.3 Cuando el TOE no supere la comprobación exigida en **CMD.1**, no debe permitir la ejecución de funciones de control con relevancia clínica, debe advertir al usuario y debe limitar la conexión con el dispositivo móvil a flujos de monitorización.

Nota de aplicación: la respuesta no debe consistir en el cierre de la aplicación cuando ello impida al paciente acceder al tratamiento; será de aplicación la conmutación prevista en **DIS.2.**

CMD.4 El TOE no debe confiar únicamente en la seguridad del sistema operativo del dispositivo móvil para ejecutar comandos con relevancia clínica, y debe implementar al menos una de las siguientes medidas: **[selección múltiple:** *ejecución de las funciones críticas en un entorno aislado por hardware con sistema operativo independiente; restricción del dispositivo móvil, mediante un motor de políticas, a un conjunto acotado de aplicaciones de confianza y de extremos de conexión; confirmación por el usuario de cada comando con relevancia clínica en la pantalla o mediante un control físico del propio dispositivo médico*].

Nota de aplicación: incluso en dispositivos móviles actualizados con frecuencia, aparecen de forma continuada vulnerabilidades explotables de severidad alta, por lo que la seguridad del sistema operativo no basta por sí sola para proteger los comandos con relevancia clínica.

CMD.5 Cuando el TOE se ejecute sobre un modelo de dispositivo móvil, una configuración o una versión de sistema operativo no incluidos en la relación de compatibilidad mantenida por el fabricante, debe actuar conforme a lo previsto en **CMD.3**. Dicha relación solo podrá incluir versiones de sistema operativo que mantengan soporte de seguridad activo.

Nota de aplicación: la relación de compatibilidad debe declararse en la Declaración de Seguridad y mantenerse actualizada por el fabricante, de forma que la publicación de nuevas versiones de sistema operativo no requiera modificar este documento. Solo se admitirá incluir versiones sin soporte de seguridad activo cuando el fabricante haya evaluado y aceptado formalmente el riesgo y lo justifique en la Declaración de Seguridad.

6. ANEXO I: TRAZABILIDAD REQUISITOS DE SEGURIDAD PARA LINCE

En la siguiente tabla se trazan qué Funciones de Seguridad definidas en el apartado 5 se considerarán aplicables en una certificación de producto a través de LINCE:

	LINCE
ADM	X
IAU	X
COM	X
CIF	X
ACT	X
AUD	X
PSC	X
PRO	X
EXP	X
FA	X
INT	X
FLU	X
ASO	X
DIS	X
CMD	X

7. ANEXO II: TRAZABILIDAD CON IEEE 2621

Para aquellos casos en los que el producto haya obtenido una certificación IEEE 2621 y que algunos requisitos de esta RFS no hayan sido incluidos en dicha certificación, se deberá llevar a cabo una **evaluación STIC complementaria**. Para determinar el conjunto de requisitos a probar en dicha evaluación, se facilita la tabla incluida en el presente anexo.

En esta tabla se traza la equivalencia entre los Requisitos Fundamentales de Seguridad definidos en el apartado 5 y los requisitos funcionales de seguridad (SFR) de la norma IEEE 2621.2, así como las prácticas recomendadas de la norma IEEE 2621.3 relativas al uso de dispositivos móviles de consumo y al mantenimiento de la disponibilidad.

Debe tenerse en cuenta que la tabla de equivalencias dependerá de las *asignaciones* y *selecciones* realizadas, tanto en la Declaración de Seguridad de la certificación IEEE 2621 como en el conjunto de requisitos a probar en la evaluación STIC complementaria. La equivalencia de requisitos deberá ser justificada y validada por el CPSMED.

Debe tenerse en cuenta que las celdas de la tabla que se encuentren vacías supondrán que la norma IEEE 2621 no incluye un requisito que satisfaga el RFS correspondiente del presente documento, que deberá verificarse en la evaluación STIC complementaria. Los SFR opcionales de IEEE 2621.2 (FIA_AFL.1, FIA_UAU.1, FIA_UAU.6 y FPT_PHP.3) solo cubrirán el RFS correspondiente cuando se hayan incluido en la Declaración de Seguridad, y las prácticas de IEEE 2621.3, al ser recomendaciones, solo cuando se haya acreditado su cumplimiento en la certificación.

Para realizar esta trazabilidad, se deberá tener en cuenta la siguiente tabla:

RFS	SFR IEEE 2621.2	Práctica recomendada IEEE 2621.3
ADM.1		
ADM.2		
ADM.3		
IAU.1	**FIA_UAU.1 (opcional)**	
IAU.2	**FIA_AFL.1 (opcional)**	
IAU.3		
IAU.4		
IAU.5		
IAU.6	**FIA_UAU.6 (opcional)**	
COM.1	**FTP_ITC.1**	
COM.2	**FTP_ITC.1**	
COM.3	**FTP_ITC.1**	

RFS	SFR IEEE 2621.2	Práctica recomendada IEEE 2621.3
COM.4		
COM.5		
COM.6	FTP_ITC.1	
COM.7		
CIF.1	FCS_COP.1	
CIF.2	FCS_COP_EXT.1.2	
ACT.1		
ACT.2	FPT_TST_EXT.1	
ACT.3		
ACT.4		
ACT.5		
ACT.6		
AUD.1		
AUD.2		
AUD.3		
AUD.4		
AUD.5		
AUD.6		
PSC.1		
PSC.2		
PSC.3		
PSC.4		
PRO.1	FPT_PHP.3 (opcional, IEEE 2621.2 §4.4.3)	
EXP.1		
EXP.2		
EXP.3		
FA.1.1		§4.1.3 §4.1.4
FA.1.2		§4.1.3 §4.1.4
FA.2		
INT.1	FDP_DAU.1.1	
INT.2	FDP_DAU.1.2	
INT.3	FDP_DAU.1	
INT.4	FPT_TST_EXT.1	
INT.5	FPT_TST_EXT.1	

RFS	SFR IEEE 2621.2	Práctica recomendada IEEE 2621.3
FLU.1	FDP_IFC.1 FDP_IFF.1.1	
FLU.2	FDP_IFF.1.2	
FLU.3	FDP_IFF.1.2 FDP_IFF.1.5	
FLU.4	FDP_IFF.1.5	
FLU.5		
ASO.1	FIA_NET_EXT.1	
ASO.2	FIA_NET_EXT.1 FTP_ITC.1	
ASO.3		
ASO.4		
ASO.5		
DIS.1		§4.1.3
DIS.2		§4.1.3
DIS.3		§4.1.4
DIS.4		§4.1.4
DIS.5		§4.1.4
DIS.6		§4.1.2 §4.1.4
DIS.7		§4.1.2 · §4.1.3
DIS.8		§4.1.3
CMD.1		§4.1.1
CMD.2		§4.1.1
CMD.3	FDP_IFF.1.5	§4.1.1
CMD.4		§4.1.2
CMD.5		§4.1.3

8. ABREVIATURAS

2FA	*Two-Factor Authentication*
AID	*Automated Insulin Dosing*
BG	*Blood Glucose*
BGM	*Blood Glucose Meter*
CCN	*Centro Criptológico Nacional*
CDD	*Connected Diabetes Devices*
CGM	*Continuous Glucose Monitor*
CPSMED	*Catálogo de Productos de Seguridad IoMT*
CPU	*Central Processing Unit*
DS	*Declaración de Seguridad*
DTLS	*Datagram Transport Layer Security*
EAL	*Evaluation Assurance Level*
ENS	*Esquema Nacional de Seguridad*
HL7	*Health Level Seven*
HTTPS	*HyperText Transfer Protocol Secure*
IEEE	*Institute of Electrical and Electronics Engineers*
IoMT	*Internet of Medical Things*
IPsec	*Internet Protocol Security*
JTAG	*Joint Test Action Group*
LE	*Low Energy (Bluetooth)*
LINCE	*Certificación Nacional Esencial de Seguridad*
MITM	*Man-In-The-Middle*
MQTT	*Message Queuing Telemetry Transport*
PAN	*Personal Area Network*
PC	*Personal Computer*
PIN	*Personal Identification Number*
PSC	*Parámetro de seguridad crítico*
PSS	*Parámetro de seguridad sensible*
RCE	*Remote Code Execution*
RFS	*Requisitos Fundamentales de Seguridad*
SFR	*Security Functional Requirements*

SFTP	*SSH File Transfer Protocol*
SSH	*Secure Shell*
STIC	*Seguridad de las Tecnologías de la Información y las Comunicaciones*
SWD	*Serial Wire Debug*
TLS	*Transport Layer Security*
TOE	*Target of Evaluation*
USB	*Universal Serial Bus*