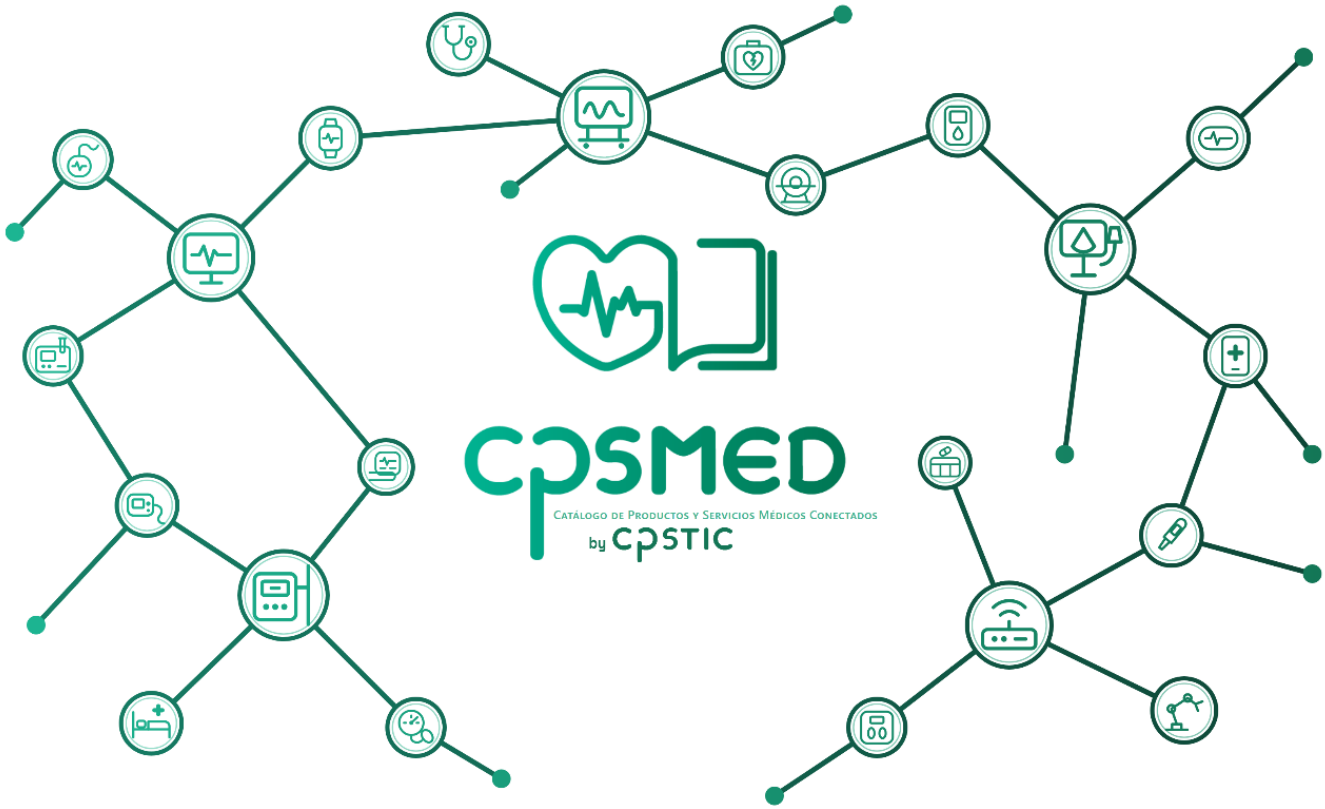
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 163

Plantilla de Procedimiento de Empleo Seguro (PES)



Noviembre 2026

Edita:

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

Versión: 1.0
Fecha de Edición: Noviembre de 2026

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

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

ÍNDICE

1 INTRODUCCIÓN 7
1.1 DESCRIPCIÓN DEL PRODUCTO 7
1.2 OBJETO Y ALCANCE 7
1.3 ORGANIZACIÓN DEL DOCUMENTO 7
2 FASE PREVIA A LA INSTALACIÓN 8
2.1 ENTREGA SEGURA DEL PRODUCTO 8
2.2 ENTORNO DE INSTALACIÓN SEGURO 8
2.3 REGISTRO Y LICENCIAS 8
2.4 CONSIDERACIONES PREVIAS 8
2.5 COMPONENTES DEL ENTORNO DE OPERACIÓN 9
3 FASE DE INSTALACIÓN 9
4 FASE DE CONFIGURACIÓN 9
4.1 MODO DE OPERACIÓN SEGURO 9
4.2 IDENTIDAD Y ACCESO 9
4.2.1 AUTENTICACIÓN 9
4.2.2 ADMINISTRACIÓN LOCAL Y REMOTA 10
4.2.3 CONFIGURACIÓN DE ADMINISTRADORES 10
4.2.4 SERVIDORES DE AUTENTICACIÓN 11
4.3 COMUNICACIONES Y CRIPTOGRAFÍA 11
4.3.1 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 11
4.3.2 GESTIÓN DE CERTIFICADOS 12
4.3.3 SINCRONIZACIÓN 12
4.4 REGISTRO Y AUDITORÍA 12
4.4.1 REGISTRO DE EVENTOS 12
4.4.2 ALMACENAMIENTO LOCAL 12
4.4.3 ALMACENAMIENTO REMOTO 12
4.5 DISPONIBILIDAD Y RESPALDO 13
4.5.1 ALTA DISPONIBILIDAD 13
4.5.2 COPIAS DE SEGURIDAD 13
4.6 ACTUALIZACIONES Y AUTO-CHEQUEOS 13
4.6.1 ACTUALIZACIONES 13
4.6.2 AUTO-CHEQUEOS 13
4.7 RESUMEN DE LA CONFIGURACIÓN SEGURA 13
5 FASE DE OPERACIÓN Y MANTENIMIENTO 15
5.1 SOPORTE DE SEGURIDAD 15
5.2 NOTIFICACIÓN DE VULNERABILIDADES 15
5.3 APLICACIÓN DE ACTUALIZACIONES DE SEGURIDAD 15
5.4 FIN DE VIDA DEL PRODUCTO 15
6 MEDIDAS A APLICAR POR LA ORGANIZACIÓN SANITARIA 15
6.1 SEGMENTACIÓN E INTEGRACIÓN EN LA RED CLÍNICA 16
6.2 INTEGRACIÓN CON SISTEMAS DE INFORMACIÓN CLÍNICA 16
6.3 GESTIÓN DEL INVENTARIO Y DEL CICLO DE VIDA 16
6.4 USO EN EL DOMICILIO DEL PACIENTE O EN MOVILIDAD 16
6.5 CONTINUIDAD ASISTENCIAL 16
7 REFERENCIAS 16
8 ABREVIATURAS 18

ÍNDICE DE TABLAS

TABLA 1: EJEMPLO TABLA5

ÍNDICE DE FIGURAS

FIGURA 1: EJEMPLO FIGURA5

INSTRUCCIONES DE CUMPLIMENTACIÓN, ENVÍO Y PUBLICACIÓN

Esta plantilla constituye el Anexo C de la CCN-STIC-163. El documento resultante de su cumplimentación será el procedimiento de empleo seguro (PES) del producto y el CCN lo publicará como guía de la serie CCN-STIC-4000, asignándole el número de guía y completando la portada, las cabeceras y la página de créditos.

El PES será distribuido por el fabricante junto con el producto y recogerá también las medidas que corresponde aplicar a la organización sanitaria durante el despliegue y la operación del producto (apartado 6).

El Anexo C de la CCN-STIC-163 se publica en formato PDF. La versión editable de la plantilla, en formato Word, puede solicitarse a través del buzón cpsmed@ccn.cni.es.

Los textos de esta plantilla son instrucciones de cumplimentación y deberán eliminarse del documento final, al igual que la tabla, la figura y la nota incluidas a título de ejemplo. Los apartados que no resulten de aplicación se mantendrán, haciendo constar expresamente su no aplicabilidad.

El solicitante remitirá la propuesta de PES, en formato editable, a la dirección cpsmed@ccn.cni.es, indicando en el asunto el nombre del producto y el código de expediente del CPSMED.

El PES se remitirá en formato Word, respetando la estructura, los estilos y los apartados de esta plantilla, de modo que el CCN pueda revisarlo y publicarlo como guía CCN-STIC de la serie 4000.

El plazo de entrega es de seis (6) meses desde la notificación del RITI favorable, conforme al apartado 4.5.5 de la CCN-STIC-163. La falta de entrega en plazo conlleva la exclusión del producto del catálogo.

El CCN revisará la propuesta y podrá devolverla con comentarios. El solicitante remitirá las versiones corregidas por el mismo canal hasta obtener la conformidad del CCN.

Obtenida la conformidad, el CCN publicará la guía, momento en el que la inclusión del producto adquiere carácter definitivo conforme al apartado 4.5.6 de la CCN-STIC-163.

Toda ampliación del alcance o nueva versión incluida que afecte al contenido del PES exigirá remitir una versión actualizada por el mismo canal, que dará lugar a una nueva edición de la guía.

Instrucciones de contenido

Deberá describirse íntegramente en este documento todo aquello que el administrador tenga que ejecutar para dejar el producto en su configuración segura: los pasos, los parámetros y los valores concretos.

Podrá referenciarse a la documentación del fabricante aquello que no condicione la configuración segura, siempre que el documento referenciado sea público y accesible, esté identificado por título, versión y fecha, se relacione en el apartado de referencias y se cite en el texto como [REFn].

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

Cuando un apartado no resulte de aplicación, se mantendrá el epígrafe y se hará constar expresamente su no aplicabilidad, justificándola.

Si el documento cubre varios modelos o plataformas y la configuración difiere entre ellos, se indicará expresamente a qué modelos aplica cada paso.

Cuando la configuración segura afecte a la operación clínica (por ejemplo, tiempos de bloqueo de sesión, alarmas o accesos de emergencia), se indicará expresamente su compatibilidad con la seguridad del paciente y con la continuidad asistencial.

Instrucciones de formato

Se emplearán los estilos de la plantilla: Título 1 a 3 para los epígrafes, Párrafo para el texto, Código para los comandos y Descripción para los pies de tabla y de figura.

Las tablas y las figuras se numerarán con su pie correspondiente y se citarán en el texto. No se emplearán cuadros de texto ni imágenes de texto, y las capturas de pantalla deberán resultar legibles.

No se modificarán la portada, las cabeceras ni los pies de página: el CCN los sustituye al publicar la guía, junto con la página de créditos y el número de la serie CCN-STIC-4000.

Las tablas, las figuras, los pies y los fragmentos de código se insertarán con el formato que se muestra a continuación.

El texto redactado por el fabricante se escribirá con el estilo Párrafo, en color negro y sin cursiva, como en el ejemplo siguiente:

Este es un ejemplo de texto de párrafo. El contenido que redacte el fabricante deberá presentar este formato, de modo que se distinga de las instrucciones de la plantilla, que figuran en gris y cursiva y deben eliminarse del documento final.

TITULOS	TITULOS
SUBTITULOS	SUBTITULOS

Tabla : Ejemplo tabla

```
Esto es texto de código
```

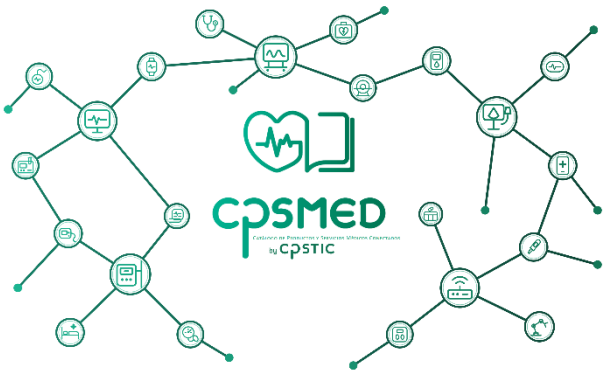


Figura : Ejemplo figura

NOTA: Ejemplo de nota, válido para todo el documento

Comprobaciones antes del envío

- *Se han eliminado todos los textos en gris y cursiva de la plantilla, incluidos los ejemplos de tabla, figura, nota y código.*
- *Se han actualizado el índice general, el índice de tablas y el índice de figuras.*
- *Los apartados que no resultan de aplicación se mantienen con su justificación.*
- *Todas las referencias citadas en el texto figuran en el apartado de referencias, con título, versión y fecha.*
- *Las capturas de pantalla son legibles y no contienen información sensible.*
- *El documento se remite en formato editable a cpsmed@ccn.cni.es.*

1 INTRODUCCIÓN

1.1 DESCRIPCIÓN DEL PRODUCTO

Descripción general del producto: finalidad prevista, componentes del sistema (dispositivo, aplicaciones, mandos, pasarelas o servidores) y caso de uso del anexo de la familia de la CCN-STIC-142 al que se refiere el procedimiento (por ejemplo, entorno hospitalario o movilidad clínica).

1.2 OBJETO Y ALCANCE

Indicar para qué producto – versión – modelos hardware – plataformas hardware – etc. se desarrolla esta guía.

El producto NOMBRE PRODUCTO ha sido incluido en el catálogo CPSMED; para conocer la familia y su criticidad, consulte el sitio web del CPSMED [REF1].

1.3 ORGANIZACIÓN DEL DOCUMENTO

a) *Apartado 2. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.*

b) *Apartado 3. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.*

c) *Apartado 4. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.*

d) *Apartado 5. En este apartado se recogen los aspectos relativos al mantenimiento seguro del producto durante su vida útil.*

e) *Apartado 6. En este apartado se recogen las medidas que corresponde aplicar a la organización sanitaria durante el despliegue y la operación del producto.*

2 FASE PREVIA A LA INSTALACIÓN

2.1 ENTREGA SEGURA DEL PRODUCTO

Describir el procedimiento de recepción segura del producto.

- *En caso de que sea un dispositivo hardware, describir paso a paso en este documento cómo verificar el embalaje externo e interno, los sellos de garantía y la correspondencia del etiquetado (marcado CE, modelo y versión) con el producto incluido en el CPSMED.*
- *En caso de que sea un producto software o incluya aplicaciones para dispositivos móviles, describir paso a paso en este documento cómo verificar la integridad y la autenticidad de la descarga (por ejemplo, firma electrónica, fichero de hash o publicación en el repositorio oficial del fabricante en la tienda de aplicaciones).*

*En caso de utilizar claves hash para la verificación de archivos, se deben utilizar **funciones SHA-256** o superiores.*

2.2 ENTORNO DE INSTALACIÓN SEGURO

Indicar si alguno de los componentes del producto (por ejemplo, servidores de gestión de dispositivos, bibliotecas de fármacos o pasarelas) debe instalarse en un Centro de Proceso de Datos (CPD), cuyo acceso estará limitado a un conjunto de personas que posean una autorización expresa. Para los dispositivos empleados en el entorno asistencial o en el domicilio del paciente, indicar las medidas de protección física recomendadas frente a la manipulación, la pérdida o el robo.

2.3 REGISTRO Y LICENCIAS

Referenciar a la documentación pública donde se describa el proceso para el registro del hardware, software y/o licencias, incluido, en su caso, el alta del dispositivo en las plataformas del fabricante y su registro en el inventario de equipamiento médico de la organización sanitaria.

2.4 CONSIDERACIONES PREVIAS

*Si fuese necesaria una configuración adicional **relativa a la seguridad, previa a iniciar la instalación y configuración** del producto, deben indicarse **paso a paso en este documento** aquellos aspectos que se deban tener en cuenta, puesto que influirán en la forma de configurarlo de forma segura.*

Por ejemplo: preparación de otros componentes necesarios (token de entropía, almacén de claves criptográficas, plataformas hardware, etc.), decisión sobre aspectos de arquitectura física (por ejemplo, alta disponibilidad), o lógica (por ejemplo, métodos de autenticación).

En el caso de productos sanitarios conectados, se considerará también la preparación de la red clínica en la que se integrará el producto (segmento o VLAN dedicada, reglas de filtrado y servicios necesarios), conforme al apartado 6.

2.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

Indicar qué componentes deben estar presentes en el entorno de operación del producto: servidor externo de autenticación, servidor externo syslog, estación de gestión, servidor de gestión de dispositivos o de bibliotecas de fármacos, sistemas de información clínica (HIS, historia clínica electrónica, prescripción electrónica) con los que se integra, dispositivos móviles compatibles, etc.

3 FASE DE INSTALACIÓN

En este apartado se hará referencia a la documentación pública donde se describa cómo llevar a cabo la instalación de cada componente del producto:

- *Dispositivo: cómo debe instalarse o verificarse el firmware correspondiente.*
- *Software: cómo se debe instalar el componente software, e indicar la plataforma sobre la que se ejecutará (servidor, workstation, etc.), incluyendo el sistema operativo y cualquier software de base que sea necesario.*
- Aplicaciones para dispositivos móviles: versiones de sistema operativo soportadas, origen de la descarga y permisos que requiere la aplicación.

*Se incluirá en este documento una indicación y descripción de los **parámetros relevantes y aspectos necesarios** para una instalación segura.*

*En caso de que el producto requiera de instalación de otros componentes adicionales, se indicará en este documento de **cuáles son y para qué se configuran**, haciendo referencia a su proceso de instalación en la documentación pública correspondiente.*

4 FASE DE CONFIGURACIÓN

4.1 MODO DE OPERACIÓN SEGURO

*Se debe **describir paso a paso en este documento** cómo activar la configuración específica del producto para que este opere en el modo de operación seguro.*

Se indicará, en su caso, cómo desactivar los modos de demostración, de servicio técnico o de fabricación que no deban estar disponibles durante la operación clínica.

4.2 IDENTIDAD Y ACCESO

4.2.1 AUTENTICACIÓN

***Describir en el documento** los mecanismos de autenticación que utiliza el producto para:*

- *Autenticación de usuarios (credenciales locales, servidor externo de autenticación, certificado, etc.).*
- *Autenticación entre componentes del producto y con servidores o dispositivos externos (certificado, claves pre-compartidas, etc.).*
- *Autenticación de sesiones (p.e SSH con clave pública, etc.).*

No se debe recomendar el uso de claves precompartidas si el producto soporta otro método (por ejemplo: certificados).

Describir los mecanismos de asociación y emparejamiento con otros dispositivos (por ejemplo, BLE o NFC con mandos remotos, sensores o aplicaciones móviles), indicando cómo autorizar y revocar las asociaciones y los parámetros de seguridad del emparejamiento.

4.2.2 ADMINISTRACIÓN LOCAL Y REMOTA

Indicar qué mecanismos se utilizarán para la administración del producto: tanto local (consola), como remota (GUI y/o CLI).

***NO** deben permitirse protocolos **inseguros** para la administración, tales como:*

- *Telnet (debe utilizarse SSH)*
- *Versión TLS inferior a 1.2 (debe utilizarse TLSv1.2 o superior)*
- *IKEv1 (debe utilizarse IKEv2)*
- *SSHv1 (debe utilizarse SSHv2)*
- *FTP (debe utilizarse SFTP o SCP)*
- *HTTP (debe utilizarse HTTPS)*

***Debe describirse paso a paso en este documento cómo desactivar los protocolos inseguros,** en caso de que sea posible. En caso de que no sea posible, debe indicarse que no se recomienda su uso.*

***Incluir una referencia a la documentación pública donde se describa cómo se configuran los protocolos seguros de administración** (por ejemplo, HTTPS/TLS, SSH).*

Describir paso a paso en este documento cómo se configuran los algoritmos y funciones criptográficas del producto, que deberán encontrarse entre los autorizados en la guía CCN-STIC-807 [REF2]. A título orientativo, la configuración de estos protocolos deberá especificarse para utilizar, únicamente, algoritmos y funciones como los siguientes:

- *DSA o RSA con claves de, al menos, 3072 bits de longitud.*
- *ECDSA con curvas P-256 o superior.*
- *Funciones Hash SHA-256 o superior.*
- *Cifrado AES-128 o superior.*
- *Grupos Diffie-Hellman 15, 16, 19, 20, 21, 28, 29 o 30.*
- *Elliptic Curve Diffie-Hellman P-256 o superior.*

*Como criterio general, **siempre que se mencione algún algoritmo de cifrado, hash o función criptográfica** en el procedimiento de empleo seguro, debe indicarse qué parámetros se utilizan. En caso de que el usuario administrador deba realizar alguna configuración para que estos sean seguros, **debe incluirse una referencia a la documentación pública donde se describa como configurarlos** (por ejemplo: cómo hacer uso de los algoritmos y funciones indicadas anteriormente, configurar las contraseñas protegidas por un valor hash o almacenamiento de backup cifrado).*

4.2.3 CONFIGURACIÓN DE ADMINISTRADORES

Incluir una referencia a la documentación del fabricante donde se describan los roles de usuario que permite el producto (por ejemplo, personal clínico, personal de electromedicina, administrador y servicio técnico del fabricante) y cómo configurarlos.

Tener en cuenta los siguientes aspectos:

- ***Configuración de la Política segura de contraseñas**. Deberá cumplir con los siguientes requisitos mínimos:*
  - *Longitud mínima de la contraseña: doce (12) caracteres.*
  - *Composición de la contraseña: letras mayúsculas, letras minúsculas, números y símbolos especiales. Recomendar el uso de los cuatro (4) grupos si el producto lo permite, y al menos un mínimo de tres (3) grupos.*
  - *Número de contraseñas anteriores que no se permite utilizar: al menos, cinco (5).*
  - *Tiempo de validez en días de las contraseñas tras el cual expiran: aproximadamente dos meses (60 días).*
  - *Número de días que deben transcurrir tras el cambio de una contraseña antes de poder modificarla de nuevo: diez (10) días.*
- ***Configuración de los parámetros de sesión.** Deberá cumplir con los siguientes requisitos mínimos:*
  - *Tiempo de inactividad de las sesiones: cinco (5) minutos.*
  - *Número de intentos fallidos de inicio de sesión: tres (3) intentos.*
  - *Tiempo de bloqueo tras los intentos fallidos: cinco (5) minutos.*
- *Configuración del mensaje de aviso y consentimiento en el inicio de sesión (**login banner**).*

Cuando alguno de estos parámetros pueda comprometer la seguridad del paciente o la continuidad asistencial (por ejemplo, el bloqueo de la interfaz clínica durante una terapia en curso), se describirá la configuración alternativa adoptada y los mecanismos de acceso de emergencia previstos, que en ningún caso permitirán modificar la configuración de seguridad.

4.2.4 SERVIDORES DE AUTENTICACIÓN

*Si el producto utiliza servidores externos de autenticación (RADIUS, LDAP, SAML, Kerberos, etc.), **hacer referencia a la documentación** que describa cómo configurarlos e indicar los parámetros relevantes para una configuración segura (por ejemplo, uso de RADSEC, LDAPv3, o TLSv1.2).*

4.3 COMUNICACIONES Y CRIPTOGRAFÍA

4.3.1 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

*En caso de que proceda, **describir paso a paso en este documento** las recomendaciones para la configuración segura de interfaces, puertos y servicios necesaria.*

Por ejemplo: deshabilitar los servicios no utilizados en el dispositivo, introducir una etiqueta que identifique el uso para el que está destinado cada interfaz, asociar a cada interfaz la dirección IP y MAC de la máquina conectada, etc.

Se indicarán los puertos y servicios necesarios para la integración con los sistemas clínicos (por ejemplo, HL7 o FHIR sobre TLS) y se deshabilitarán las interfaces de servicio técnico (USB, puertos serie o de depuración) que no sean necesarias durante la operación.

4.3.2 GESTIÓN DE CERTIFICADOS

*Deben **indicarse** los algoritmos y funciones criptográficas del producto que cumplan con las especificaciones de la guía CCN-STIC-807 y **hacer referencia a la documentación pública** donde se describa cómo configurarlos. Estos parámetros son:*

- *RSA con claves de, al menos, 3072 bits de longitud.*
- *ECDSA con curvas P-256 o superior.*
- *DSA con claves de, al menos, 3072 bits de longitud.*
- *Funciones Hash SHA-256 o superior.*

*Se deberá **hacer referencia a la documentación** donde se describa cómo hacer la solicitud de certificado (CSR), importar el certificado de servidor, importar los certificados de CAs y otros parámetros necesarios.*

4.3.3 SINCRONIZACIÓN

***Incluir referencia a la documentación pública** donde se describa cómo debe configurarse la sincronización segura del producto y sus componentes. Se debe recomendar **la integración con servicio NTP** en caso de que sea posible y cómo activar la autenticación en caso de que sea posible.*

4.4 REGISTRO Y AUDITORÍA

4.4.1 REGISTRO DE EVENTOS

***Hacer referencia a la documentación pública** donde se indique qué eventos se registran y cómo se efectúa el registro. Por ejemplo: fichero de logs de configuración, fichero de logs de sistema, etc.*

Indicar el formato de los registros de log, incluyendo un ejemplo de estos.

Los registros no incluirán datos de salud de los pacientes más allá de los estrictamente necesarios para la trazabilidad de los eventos de seguridad.

4.4.2 ALMACENAMIENTO LOCAL

***Hacer referencia a la documentación pública** donde se describa cómo funciona el almacenamiento local de registros de auditoría en el producto.*

En caso de que fuera necesaria alguna configuración para el almacenamiento seguro de registros, describir en este documento.

4.4.3 ALMACENAMIENTO REMOTO

***Hacer referencia a la documentación pública donde se indique** cómo se configura el envío de registros a un servidor remoto syslog y cómo se configura este. Deberá utilizarse siempre un protocolo seguro para el envío de los registros (Por ejemplo, TLSv1.2 o IPsec).*

4.5 DISPONIBILIDAD Y RESPALDO

4.5.1 ALTA DISPONIBILIDAD

__Hacer referencia la documentación pública__ donde se describa la configuración de alta disponibilidad del producto. Indicar en este documento los parámetros de configuración necesarios para una configuración segura.

Describir el comportamiento del producto ante la pérdida de conectividad o la indisponibilidad de los sistemas externos (funcionamiento autónomo), las alarmas que se generan y su configuración.

4.5.2 COPIAS DE SEGURIDAD

Deben indicarse los componentes, datos y configuraciones sobre las que han de realizarse los backups.

__Hacer referencia a la documentación pública__ donde describa el proceso de configuración y realización de las copias de seguridad de forma segura.

Se debe recomendar la realización de backups periódicos.

En particular, se indicará cómo respaldar y restaurar de forma segura la biblioteca de fármacos, los parámetros terapéuticos y la configuración del producto.

4.6 ACTUALIZACIONES Y AUTO-CHEQUEOS

4.6.1 ACTUALIZACIONES

__Hacer referencia a la documentación__ donde se describa el proceso a seguir para realizar actualizaciones de firmware, software, servicios, etc. de forma segura.

En caso de que sea necesario, se debe indicar en este documento el uso de protocolos seguros como SCP o SFTP y hacer referencia a la documentación donde se describa cómo configurarlos. Se indicará asimismo cómo se verifica la autenticidad e integridad del paquete de actualización antes de su instalación y cómo se impide la actualización durante una terapia en curso. La política de actualizaciones de seguridad se describe en el apartado 5.3.

4.6.2 AUTO-CHEQUEOS

Describir los auto-chequeos (self-test) de integridad del software y de la operación de los algoritmos y funciones criptográficas, indicar cuándo los realiza (en el arranque o bajo demanda del administrador) y qué ocurre en caso de fallo, en particular su efecto sobre la función clínica y las alarmas que se generan.

4.7 RESUMEN DE LA CONFIGURACIÓN SEGURA

Incluir un cuadro resumen con los parámetros de seguridad configurados y el valor establecido en cada uno, indicando el apartado de este documento en el que se describe su configuración.

Parámetro	Valor configurado	Apartado
[Parámetro de seguridad]	*[Valor establecido]*	*[4.x]*

5 FASE DE OPERACIÓN Y MANTENIMIENTO

En este apartado se recogen los aspectos relativos al mantenimiento seguro del producto durante su vida útil.

5.1 SOPORTE DE SEGURIDAD

Indicar el periodo de soporte de seguridad de la versión incluida en el CPSMED, la vida útil declarada del producto sanitario y la fecha prevista de fin de soporte. El periodo de soporte de seguridad no podrá ser inferior a cinco (5) años desde la fecha de inclusión del producto en el CPSMED, conforme al compromiso asumido en la declaración responsable (FOR-CPSMED-01) de la CCN-STIC-163. El fabricante está obligado a notificar al CPSMED la finalización del soporte de seguridad, conforme a lo establecido en la CCN-STIC-163.

5.2 NOTIFICACIÓN DE VULNERABILIDADES

Indicar el canal de notificación de vulnerabilidades del fabricante, los plazos de respuesta comprometidos y el medio por el que se comunican los avisos de seguridad a los usuarios del producto, así como su coordinación con el sistema de vigilancia de productos sanitarios (avisos de seguridad y acciones correctivas de seguridad en campo, FSCA, comunicadas a la AEMPS).

5.3 APLICACIÓN DE ACTUALIZACIONES DE SEGURIDAD

Describir la política de actualizaciones de seguridad: periodicidad, verificación de la autenticidad e integridad de los paquetes antes de su instalación y efecto de la actualización sobre la configuración segura descrita en este documento. La configuración del mecanismo de actualización se describe en el apartado 4.6.1.

5.4 FIN DE VIDA DEL PRODUCTO

Describir el procedimiento de borrado seguro de la información, los datos de salud de los pacientes, las credenciales y el material criptográfico almacenados en el producto antes de su retirada, devolución, envío a reparación o reasignación a otro paciente o servicio.

6 MEDIDAS A APLICAR POR LA ORGANIZACIÓN SANITARIA

En este apartado se recogen las medidas que, sin formar parte de los RFS del producto, corresponde aplicar a la organización sanitaria durante el despliegue y la operación del producto para mantener su configuración segura, conforme a la CCN-STIC-142 [REF4] y a la norma IEC 80001-1 [REF5].

El fabricante describirá estas medidas con el nivel de detalle necesario para que la organización sanitaria pueda aplicarlas, indicando cuáles resultan imprescindibles para el uso seguro del producto.

6.1 SEGMENTACIÓN E INTEGRACIÓN EN LA RED CLÍNICA

Describir la arquitectura de red recomendada para el despliegue del producto: segmentación de la red clínica (segmento o VLAN dedicada), flujos de comunicación permitidos con otros sistemas, puertos y protocolos necesarios y reglas de filtrado que debe aplicar la organización sanitaria.

6.2 INTEGRACIÓN CON SISTEMAS DE INFORMACIÓN CLÍNICA

Describir la integración segura con los sistemas de información clínica (HIS, historia clínica electrónica, prescripción electrónica, centrales de monitorización), indicando los protocolos empleados (por ejemplo, HL7 o FHIR sobre TLS), la autenticación entre sistemas y las responsabilidades de la organización sanitaria en su configuración.

6.3 GESTIÓN DEL INVENTARIO Y DEL CICLO DE VIDA

Indicar la información que la organización sanitaria debe registrar en su inventario de equipamiento médico o GMAO (modelo, versión de firmware y software, ubicación y asociaciones con otros dispositivos) y cómo debe gestionar las actualizaciones, los avisos de seguridad del fabricante y la retirada del producto.

6.4 USO EN EL DOMICILIO DEL PACIENTE O EN MOVILIDAD

Cuando el producto se emplee fuera del centro sanitario (caso de uso de movilidad clínica), describir las indicaciones que deben facilitarse al paciente o cuidador: protección física del dispositivo, emparejamiento únicamente con dispositivos autorizados, uso de dispositivos móviles de consumo compatibles y actualizados, y actuación en caso de pérdida o robo.

6.5 CONTINUIDAD ASISTENCIAL

Describir las medidas que debe prever la organización sanitaria para mantener la asistencia ante un incidente de seguridad o la indisponibilidad del producto o de los sistemas con los que se integra (procedimientos alternativos, equipos de respaldo y notificación del incidente al fabricante y a las autoridades competentes).

7 REFERENCIAS

Indicar documentación que se haya referenciado a lo largo de la guía.

REF1	CPSMED https://cpsmed.ccn.cni.es
REF2	CCN-STIC-807 Criptología de empleo en el Esquema Nacional de Seguridad.
REF3	Guía CCN-STIC-163 y sus anexos.
REF4	CCN-STIC-142 Taxonomía de referencia para productos y servicios médicos conectados (IoMT) y anexo de RFS de la familia.

REF5 IEC 80001-1:2021 Application of risk management for IT-networks incorporating medical devices – Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software.

REF6 Reglamento (UE) 2017/745 sobre los productos sanitarios (MDR) y Reglamento (UE) 2017/746 sobre los productos sanitarios para diagnóstico in vitro (IVDR).

8 ABREVIATURAS

AEMPS	Agencia Española de Medicamentos y Productos Sanitarios.
BLE	Bluetooth de baja energía (Bluetooth Low Energy).
CA	Autoridad de certificación (Certification Authority).
CLI	Interfaz de línea de comandos (Command Line Interface).
CPD	Centro de Proceso de Datos.
CPSMED	Catálogo de Productos y Servicios Médicos Conectados.
CSR	Solicitud de firma de certificado (Certificate Signing Request).
ENS	Esquema Nacional de Seguridad.
FHIR	Fast Healthcare Interoperability Resources.
FSCA	Acción correctiva de seguridad en campo (Field Safety Corrective Action).
GMAO	Gestión del Mantenimiento Asistido por Ordenador.
GUI	Interfaz gráfica de usuario (Graphical User Interface).
HIS	Sistema de información hospitalaria (Hospital Information System).
HL7	Health Level Seven.
IoMT	Internet de las cosas médicas (Internet of Medical Things).
LDAP	Protocolo ligero de acceso a directorios (Lightweight Directory Access Protocol).
MDR	Reglamento (UE) 2017/745 sobre los productos sanitarios (Medical Devices Regulation).
NFC	Comunicación de campo cercano (Near Field Communication).
NTP	Protocolo de tiempo de red (Network Time Protocol).
PES	Procedimiento de Empleo Seguro.
RADIUS	Remote Authentication Dial-In User Service.
SAML	Security Assertion Markup Language.
SSH	Secure Shell.
TLS	Seguridad de la capa de transporte (Transport Layer Security).
VLAN	Red de área local virtual (Virtual Local Area Network).