PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DEL SUMINISTRO DE 18 MONITORES DESFIBRILADORES PARA EL CENTRO DE EMERGENCIAS SANITARIAS 061

El redactor

Ignacio García Delgado

Subdirección Económico-Administrativa y Servicios Generales

Es copia auténtica de documento electrónico

ÍNDICE

Es copia auténtica de documento electrónico

Es copia auténtica de documento electrónico

Puede verificar la integridad de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	FRANCISCO POZO MUÑOZ	27/02/2026
VERIFICACIÓN	Pk2jmJDYWKKLFP3HRTUGDTKAF4D7YC	PÁG. 4/40

Es copia auténtica de documento electrónico

1. OBJETO DEL CONTRATO

El presente contrato tiene por objeto el suministro de dieciocho (18) unidades de monitores desfibriladores, con destino a los equipos de emergencias del Centro de Emergencias Sanitarias 061 (CES 061), con el fin de reforzar la respuesta asistencial ante situaciones de soporte vital avanzado (SVA) y la capacidad diagnóstica y toma de decisiones clínicas en situaciones de urgencia y emergencia en el entorno extrahospitalario.

Lote	Código SAS	GC	Descripción
1	SU.EQ.ELEC.03.02.08	F47552	Monitor desfibrilador – Compacto

El CES 061 está estructurado territorialmente en una Sede Central y ocho Servicios Provinciales, uno por cada provincia andaluza, y dispone de centros coordinadores y bases asistenciales que operan de forma ininterrumpida las 24 horas del día, todos los días del año. Esta estructura funcional exige la disponibilidad permanente de equipamiento médico adecuado, especialmente en situaciones críticas, siendo por ello prioritaria la dotación de dispositivos eficaces, seguros y adaptados a las condiciones operativas del medio prehospitalario.

Los monitores-desfibriladores objeto del suministro deberán estar diseñados específicamente para su uso en el ámbito de las urgencias y emergencias extrahospitalarias, garantizando un funcionamiento seguro, fiable y continuado en escenarios de alta exigencia operacional.

Deberán cumplir los requisitos técnicos, de seguridad eléctrica y de calidad establecidos en la normativa nacional e internacional vigente.

Asimismo, los equipos deberán estar alineados con las recomendaciones clínicas publicadas en las Guías ERC 2025, basadas en el consenso internacional ILCOR 2025, especialmente en lo relativo a:

- Desfibrilación precoz con mínima interrupción del masaje cardíaco.
- Optimización de la calidad de la RCP, incluyendo feedback objetivo de profundidad, frecuencia, retroceso torácico y fracción de compresiones (CCF).
- Tecnologías destinadas a reducir las pausas peri-choque, tales como el análisis durante compresiones, filtrado avanzado del artefacto de RCP o sistemas equivalentes.
- Sincronización precisa en cardioversión y disponibilidad de modos de estimulación (pacing) adecuados a las recomendaciones clínicas vigentes.

El diseño del equipo, sus baterías, accesorios, cables, soportes de ambulancia y cargadores deberá ser adecuados para el entorno extrahospitalario, garantizando resistencia mecánica, protección ambiental (polvo/agua), estabilidad térmica y la autonomía necesaria para intervenciones prolongadas, conforme a las necesidades asistenciales del SSPA.

El contrato incluye el suministro de todos los accesorios necesarios para el uso y funcionalidad completa de los equipos, incluyendo, en su caso, cables, baterías, sistemas de carga y fundas de protección.

La empresa adjudicataria deberá realizar la entrega técnica de los equipos en presencia del personal

Es copia auténtica de documento electrónico

designado por el CES 061, procediendo a su puesta en funcionamiento y verificando su correcto estado operativo y funcional, tras lo cual se emitirá un acta de recepción conforme firmada por ambas partes.

Asimismo, el adjudicatario deberá impartir formación específica al personal sanitario del CES 061 para el correcto uso y mantenimiento del equipamiento suministrado, en las fechas y condiciones que determine la planificación formativa del centro, de conformidad con lo previsto en el apartado 7 de este Pliego.

2. REQUISITOS DEL SUMINISTRO

Los monitores desfibriladores suministrados deberán ser:

- Equipos nuevos de fábrica.
- Año de fabricación no anterior a un año desde la publicación del pliego.
- De la misma marca, modelo, versión y configuración.
- Estar provistos de todos los accesorios necesarios para su utilización adecuada y su correcta ubicación y fijación en ambulancias clase C del CES 061.

El suministro incluirá, los accesorios y fungibles necesarios para el uso completo y seguro del equipo conforme a su funcionalidad declarada.

Con objeto de facilitar la verificación técnica y la correcta valoración de las ofertas, el licitador deberá presentar la información y documentación técnica indicada en el Anexo I de este documento.

3. ESPECIFICACIONES TÉCNICAS

La atención inicial a procesos tiempo-dependientes (como la parada cardiorrespiratoria, las arritmias potencialmente letales, el compromiso de la ventilación, la perfusión ineficaz o el shock) exige una respuesta inmediata, coordinada y basada en la utilización de equipamiento clínico avanzado, capaz de garantizar la monitorización continua y la aplicación segura de terapias de Soporte Vital Avanzado.

En este contexto, los monitores desfibriladores constituyen un recurso asistencial esencial, ya que permiten la evaluación en tiempo real del estado hemodinámico y respiratorio del paciente, el diagnóstico precoz de trastornos del ritmo y la administración rápida y eficaz de desfibrilación, cardioversión y estimulación cardíaca externa.

Dado que estas intervenciones se realizan en entornos extrahospitalarios altamente exigentes, el equipamiento debe estar específicamente diseñado para su uso en urgencias y emergencias, ofreciendo:

- Fiabilidad operativa en escenarios críticos.
- Robustez estructural y resistencia ambiental.
- Rapidez en la aplicación de terapias eléctricas.
- Monitorización avanzada de constantes vitales.
- Integración funcional con los procedimientos clínicos y operativos del SVA.

Las presentes especificaciones técnicas definen las características mínimas que deben cumplir los monitores-desfibriladores objeto del suministro, con el fin de garantizar la seguridad del paciente, la calidad asistencial y la adecuación al entorno operativo del SSPA.

Es copia auténtica de documento electrónico

3.1. REQUISITOS TÉCNICOS MÍNIMOS DEL LOTE DE MONITORES DESFIBRILADORES

A continuación, se detallan los requisitos técnicos mínimos que deberán cumplir los equipos a suministrar.

Definición del equipo

Equipo médico portátil, de diseño modular o compacto, destinado al soporte vital avanzado (SVA). Integra en un único dispositivo las terapias cardíacas esenciales (desfibrilación, cardioversión y marcapasos transcutáneo) junto con un sistema completo de monitorización multiparamétrica: ECG de 12 derivaciones, ritmo cardíaco, pulsioximetría, capnografía, presión arterial no invasiva, tendencias y herramientas de apoyo a la RCP.

Está indicado para su uso en pacientes adultos, pediátricos y neonatos, y apto para su uso en vehículos de emergencias terrestres y aéreos.

3.1.1. General

3.1.1.1. Perfil de pacientes

El equipo deberá permitir la atención integral al paciente: Neonatal, pediátrico y adulto

Pudiendo ajustar límites de alarma, parámetros de energía y modos de monitorización en función de la selección de paciente.

3.1.1.2. Funcionamiento

El equipo debe funcionar en:

- Modo DEA/Semiautomático
- Modo Manual (selección nivel de energía, desfibrilación, marcapasos y cardioversión)

3.1.1.3. Funda de transporte

El equipo deberá suministrarse con funda de transporte específica del fabricante, diseñada para uso intensivo en emergencias extrahospitalarias y que cumpla:

- Bolsillos de fácil acceso para cables, sensores y parches.
- Protección integral del equipo frente a golpes y rozaduras.
- Disposición organizada de los accesorios para manipulación rápida.
- Correas, asas o arnés para transporte ergonómico y seguro.
- Reparto equilibrado de la carga según la configuración del dispositivo.

3.1.2. Robustez orientada al medio prehospitalario

El monitor-desfibrilador deberá estar específicamente diseñado para su uso en el entorno extrahospitalario, garantizando un funcionamiento seguro, estable y continuo ante las condiciones mecánicas, térmicas, ambientales y operativas propias del transporte sanitario.

Para acreditar dicho cumplimiento, el licitador deberá cumplir las especificaciones que se detallan a continuación, relativas a la marca, modelo y versión ofertada:

Norma UNE-EN 1789: Vehículos de transporte sanitario y equipamiento médico a bordo

Norma de referencia para la seguridad e integración del equipo en la ambulancia.

Es copia auténtica de documento electrónico

El licitador dispondrá de certificado o informe de ensayo que el equipo, conjuntamente con su sistema de fijación/anclaje ofertado, cumple con los requisitos de retención y resistencia a impactos establecidos en la norma vigente.

Norma IEC 60601-1: Seguridad básica y funcionamiento esencial de equipos electromédicos

Norma internacional que regula la seguridad eléctrica, mecánica, térmica y los requisitos de funcionamiento esencial de equipos electromédicos.

El licitador dispondrá de declaración del fabricante o certificado de ensayo que acredite el cumplimiento íntegro de esta norma en el modelo ofertado.

Cumplimiento de la norma IEC 60601-1-2: Compatibilidad electromagnética (EMC)

Regula la inmunidad del equipo frente a interferencias y su capacidad para no emitir perturbaciones

El licitador dispondrá de certificación del cumplimiento de EMC conforme a IEC 60601-1-2 vigente, asegurando la no interferencia con otros dispositivos.

Cumplimiento de la norma IEC 60601-1-12: Equipos electromédicos para emergencias médicas

Norma específica y obligatoria para equipos utilizados en condiciones extremas fuera del entorno hospitalario controlado. Esta norma engloba y exige los ensayos de resistencia mecánica y ambiental.

El licitador dispondrá de certificado oficial del cumplimiento de la IEC 60601-1-12, acreditando específicamente la resistencia a:

- **Vibración mecánica:** (Aleatoria y Sinusoidal) garantizando la integridad estructural y funcional tras la exposición prolongada a vibraciones propias del transporte terrestre y aéreo.
- **Choque y caída libre:** Resistencia a impactos mecánicos durante el uso portátil.
- **Condiciones ambientales:** Funcionamiento bajo condiciones de humedad y temperatura variables.

Grado de protección IP55: Protección frente a polvo y chorros de agua

El equipo deberá disponer de un grado de protección IP55 como mínimo, garantizando:

- **IP 5X (polvo):** Protección frente a entrada de polvo suficiente para evitar interferencias en el funcionamiento del equipo.
- **IP X5 (agua):** Resistencia a chorros de agua proyectados desde cualquier ángulo. Garantiza el uso seguro en exteriores, lluvia intensa, limpieza del equipo y entornos mojados o contaminados.

Declaración UE de conformidad del fabricante y Fichas Técnicas oficiales

El equipo dispone de:

- Declaración UE de conformidad emitida por el fabricante.
- Fichas técnicas oficiales correspondientes al modelo, versión y configuración ofertada.

Ambos documentos garantizarán la trazabilidad normativa, el marcado CE y la conformidad legal del dispositivo en la Unión Europea.

Funcionamiento del equipo: Rango operativo entre 0 y 45 °C

El monitor-desfibrilador deberá garantizar funcionamiento seguro y estable dentro del rango

Es copia auténtica de documento electrónico

ambiental habitual del entorno extrahospitalario.

El equipo debe acreditar un rango operativo entre 0 °C y 45 °C, tanto para el equipo como para la electrónica interna, asegurando:

- Arranque estable en frío.
- Tolerancia a temperaturas elevadas en vehículo.
- Continuidad asistencial en condiciones térmicas adversas.

3.1.3. Características físicas orientadas a la ergonomía del transporte y funcionalidad en la ambulancia

El monitor-desfibrilador deberá presentar unas dimensiones y un peso acordes a las exigencias operativas del entorno extrahospitalario, facilitando su transporte manual, su manipulación en espacios reducidos y su correcta instalación o uso dentro del habitáculo asistencial de la ambulancia.

3.1.3.1. Peso máximo del equipo en configuración completa (≤ 9,5 kg)

Requisito:
El peso total no superará los 9,5 kg en configuración completa.

3.1.4. Visualización de datos: Pantalla e Impresora

El monitor-desfibrilador deberá integrar un sistema de visualización de alto rendimiento diseñado específicamente para el entorno prehospitalario, asegurando una lectura nítida, rápida y fiable bajo cualquier condición de iluminación (oscuridad total a luz solar directa).

3.1.4.1. Pantalla

Tecnología y Tamaño: La unidad dispondrá de una pantalla color (TFT, LCD, LED o tecnología superior) con un tamaño diagonal mínimo de 6,5 pulgadas.

Visibilidad en exteriores: El equipo deberá garantizar la legibilidad de las curvas y datos a la luz solar directa.

Capacidad de visualización: Deberá permitir la visualización simultánea de, al menos, 3 curvas fisiológicas (ondas) en tiempo real, junto con los valores numéricos de los parámetros monitorizados.

Configuración: Deberá permitir el ajuste de la velocidad de barrido (al menos 25 mm/s y 50 mm/s) para facilitar el análisis detallado del trazado.

Interacción: En caso de incorporar pantalla táctil, esta deberá ser operativa con guantes de nitrilo/látex y resistente a salpicaduras. Si es táctil, deberá disponer de teclas físicas o dial de navegación redundante para garantizar la operatividad en caso de fallo del táctil o condiciones de suciedad extrema.

3.1.4.2. Calidad diagnóstica

El sistema deberá garantizar la capacidad de realizar un diagnóstico clínico preciso de alteraciones del ritmo y de la morfología del ECG (ondas P, complejos QRS, segmento ST, ondas T).

3.1.4.3. Requisitos en Pantalla y/o Impresora:

El equipo deberá cumplir con los siguientes requisitos en Pantalla y/o Impresora:

- **Ancho de banda diagnóstico:** El equipo deberá disponer de un modo de filtrado "Diagnóstico" con un ancho de banda de frecuencias de al menos 0,05 Hz a 150 Hz (o rango

Es copia auténtica de documento electrónico

equivalente según norma IEC 60601-2-27), permitiendo la impresión o visualización sin distorsión del segmento ST.

- **Resolución de trazado:** La resolución de la pantalla deberá ser 1024x768 píxeles o superior, para identificar claramente alteraciones morfológicas.
- **Impresora:**
  - El equipo integrará una impresora térmica de alta resolución.
  - Deberá permitir la impresión de tiras de ritmo y de 12 derivaciones.
  - Ancho de papel mínimo 80 mm
  - Velocidades de impresión configurables (mínimo 25 mm/s).
  - La impresión deberá tener calidad diagnóstica certificada, sirviendo como documento médico legal del evento.

El licitador aportará ficha técnica donde se especifique el tamaño de pantalla, la tecnología de visualización bajo luz solar, pixeles y ancho de banda (frecuencia) para modo diagnóstico.

3.1.5. Parámetros de monitor

El monitor-desfibrilador deberá permitir la monitorización avanzada y continua de los parámetros esenciales en Soporte Vital Avanzado, garantizando exactitud, estabilidad de señal y funcionamiento fiable en entorno extrahospitalario. El equipo deberá integrar, como mínimo, los siguientes módulos o capacidades:

A. DESFIBRILACIÓN

El equipo deberá permitir desfibrilación mediante onda bifásica, con un rango de energía ajustable entre 2 y 200 J, asegurando la corrección automática de impedancia torácica.

La administración del choque deberá realizarse exclusivamente mediante electrodos multifunción válidos para paciente adulto, pediátrico y neonatal.

El sistema debe disponer de los siguientes modos operativos:

- Manual
- Automático / semiautomático (DEA)
- Sincronizado (cardioversión)

El licitador deberá garantizar que los tiempos de carga y descarga son adecuados para un entorno de emergencias.

B. CARDIOVERSIÓN

El dispositivo deberá permitir cardioversión sincronizada, con detección fiable de complejo QRS, y cardioversión asincrónica cuando la situación clínica lo requiera.

C. MARCAPASOS TRANSCUTÁNEO

El monitor-desfibrilador deberá disponer de estimulación cardíaca externa, en modo a demanda y no demanda, con capacidad de ajustar la frecuencia en un rango de, al menos, 40 a 170 ppm, así como regulación de intensidad según respuesta mecánica del paciente.

D. ELECTROCARDIOGRAFÍA (ECG)

Es copia auténtica de documento electrónico

El equipo deberá permitir:

- Registro e interpretación de al menos 12 derivaciones.
- Visualización continua del ECG con calidad diagnóstica.
- Mediciones básicas automáticas del ECG (intervalos y segmentos).

E. PULSIOXIMETRÍA (SPO_2)

El monitor-desfibrilador debe integrar un sistema de pulsioximetría avanzado que garantice una medición precisa, estable y continua en las condiciones críticas del entorno extrahospitalario: movimiento, baja perfusión/shock y uso pediátrico.

El sistema deberá permitir:

- La visualización en tiempo real de la onda pletismográfica, como indicador de calidad de señal, perfusión periférica y detección de artefactos.

El licitador deberá disponer de la documentación técnica o certificación del fabricante que acredite que el sistema ofertado presenta estas prestaciones de tecnologías empleadas en emergencias extrahospitalarias en escenarios de baja perfusión.

F. CAPNOGRAFÍA (CO_2)

El monitor-desfibrilador deberá permitir la medición de CO_2 espirado en:

- Paciente intubado (capnografía convencional)
- Paciente no intubado (capnografía de vía aérea no invasiva)

Deberá incluir la visualización continua de la onda de CO_2 y el valor numérico del $ETCO_2$.

G. PRESIÓN ARTERIAL NO INVASIVA (PANI)

El equipo deberá ofrecer medición automática de presión arterial no invasiva, con un rango de medición mínimo de:

- Presión sistólica: 40 – 250 mmHg
- Presión diastólica: 20 – 200 mmHg

Se deberá permitir la configuración de intervalos automáticos de medida y medición manual inmediata.

3.1.6. Sistema de calidad y ayuda a la reanimación cardiopulmonar durante la asistencia.

El monitor-desfibrilador deberá integrar un sistema avanzado de asistencia a la RCP que proporcione retroalimentación objetiva y en tiempo real sobre la calidad de las compresiones torácicas realizadas por el personal asistencial.

Requisitos de la funcionalidad:

- **Activación:** La funcionalidad deberá estar totalmente operativa y con licencia de forma permanente en la configuración ofertada.
- **Medición:** La medición se realizará mediante sensor integrado en electrodos de desfibrilación y/o mediante dispositivo acelerómetro que se conecte al equipo.

Capacidades de monitorización y ayuda en tiempo real:

Es copia auténtica de documento electrónico

El equipo deberá guiar al personal asistencial visual y/o acústicamente a cumplir con las recomendaciones internacionales vigentes (ERC/AHA), monitorizando al menos:

- **Frecuencia de compresiones:** Incluyendo metrónomo integrado.
- **Profundidad de las compresiones:** Indicación de si la compresión es insuficiente o excesiva.
- **Retorno torácico:** Aviso en caso de que no se permita la reexpansión completa del tórax.
- **Tiempos de inactividad:** Avisos para minimizar las pausas sin compresiones

Resumen post-evento:

El monitor deberá permitir la visualización en su propia pantalla, de forma inmediata tras finalizar el caso, de un resumen de los datos del evento (Tiempo total de RCP, fracción de compresión, promedios de frecuencia/profundidad) para permitir una valoración clínica rápida in situ, sin necesidad de volcar datos a un ordenador externo en ese momento.

3.1.7. Alimentación

El monitor-desfibrilador deberá funcionar de manera autónoma mediante baterías recargables de ion-litio, y deberá poder cargarse a través de una fuente de alimentación externa conforme a los estándares operativos del entorno extrahospitalario.

A. Alimentación eléctrica

El equipo deberá incluir sistemas de alimentación que permitan:

- Funcionamiento y carga simultánea desde fuentes externas.
- Compatibilidad con:
    - Corriente continua (CC) a 12 V, apta para vehículos de emergencias.
    - Corriente alterna (CA) a 220 V, apta para bases y puntos de recarga.

Los adaptadores incluidos deberán permitir la carga completa de las baterías y el funcionamiento del monitor mientras está conectado a la fuente externa.

B. Autonomía

El monitor-desfibrilador deberá garantizar la siguiente autonomía mínima, en condiciones de monitorización continua de los parámetros requeridos:

Equipos con más de una batería:

- Autonomía mínima: 9 horas (para el total de las baterías)

Equipos con una única batería:

- Autonomía mínima: 6 horas.

Además, independientemente del número de baterías instaladas, el equipo deberá ser capaz de realizar al menos 200 descargas a 200 julios sin comprometer su operatividad.

El licitador dispondrá de la documentación técnica del fabricante que acredite los valores de autonomía y capacidad de descarga bajo las condiciones especificadas.

3.1.8. Soporte de ambulancia

El monitor-desfibrilador deberá disponer de un soporte cargador de pared de 12 V, apto para

Es copia auténtica de documento electrónico

ambulancias de clase C, que permita el anclaje y desanclaje rápido del equipo, garantizando un uso seguro, estable y compatible con las condiciones dinámicas del entorno extrahospitalario.

El soporte deberá cumplir los requisitos de instalación y seguridad establecidos en la norma UNE-EN 1789, que exige que todo equipamiento montado en ambulancias (monitor, respirador, bomba, cargador o soporte) disponga de certificación conforme a dicha norma, incluyendo:

- Resistencia a fuerzas de 10 G en cuatro direcciones, garantizando la integridad del equipo durante aceleraciones, frenadas y colisiones.
- Fijación permanente y certificada, que asegure una sujeción robusta y estable al vehículo.
- Ensayos de conformidad con UNE-EN 1789 junto con los requisitos de IEC 60601-1-12, que avalen su uso en entornos móviles, con vibración, impacto y temperaturas extremas.

El licitador dispondrá de la certificación oficial del fabricante o laboratorio acreditado que acredite el cumplimiento del soporte con las normas mencionadas.

3.1.9. Prestaciones clínicas enfocadas a la asistencia del paciente crítico en emergencias

El monitor-desfibrilador deberá integrar un conjunto de prestaciones clínicas orientadas a la valoración, seguimiento y toma de decisiones en pacientes críticos en el entorno prehospitalario, facilitando la detección precoz de deterioro y la monitorización avanzada durante la asistencia.

El equipo deberá cumplir, como mínimo, los siguientes requisitos:

- Predicción o detección temprana de deterioro, mediante análisis continuo de los parámetros monitorizados y presentación de alertas o indicadores basados en tendencias o variaciones significativas.
- Registro y visualización de tendencias en los parámetros monitorizados (ECG, SpO_2, CO_2, PANI, frecuencia cardíaca, frecuencia respiratoria), con representación gráfica y numérica.
- Capacidad de ampliación funcional, que permita incorporar nuevas opciones de medición o funcionalidades avanzadas mediante módulos, accesorios o actualizaciones de software compatibles con el equipo.

El licitador dispondrá de certificado o declaración del fabricante que acredite que el equipo está diseñado para permitir la integración futura de estas ampliaciones.

3.1.10. Conectividad

El monitor-desfibrilador deberá disponer de los medios de conectividad inalámbrica necesarios para permitir la comunicación de datos clínicos conforme a lo establecido en el apartado 3.1.11 (Tratamiento de datos e integración clínica), sin requerir software, licencias, servicios externos o plataformas adicionales que generen coste para el órgano de contratación.

El equipo deberá incorporar, como mínimo, los siguientes modos de conexión:

- Telefonía móvil: 4G o 5G
- WiFi
- Bluetooth

A. Alarmas

Es copia auténtica de documento electrónico

El monitor deberá disponer de alarmas configurables visuales y audibles, ajustables según criterio del profesional.

B. Comunicación

El equipo deberá permitir el uso de los modos de conectividad integrados para el envío y recepción de datos clínicos definidos en el apartado 3.1.11 (Tratamiento de datos e integración clínica), sin necesidad de sistemas externos adicionales.

C. Monitores Desfibriladores modulares (cuando aplique)

En equipos con arquitectura modular, el fabricante deberá garantizar que:

- La comunicación entre módulos es estable, continua y segura,
- Opera en condiciones de movimiento y vibración propias del entorno extrahospitalario,
- No requiere hardware adicional fuera del equipamiento ofertado.

El licitador dispondrá de documentación técnica que describa el mecanismo de comunicación interna entre módulos.

3.1.11. Tratamiento de datos e integración clínica

El monitor-desfibrilador deberá permitir la transmisión, registro e integración en tiempo real de la información clínica generada durante la asistencia extrahospitalaria, garantizando la interoperabilidad con los sistemas corporativos del SSPA.

A. TRANSMISIÓN Y REGISTRO DE INFORMACIÓN

El equipo deberá permitir:

- Transmisión en tiempo real de:
    - ECG y trazados
    - Constantes vitales
    - Capnografía
    - Eventos e intervenciones
- Interacción bidireccional entre el monitor-desfibrilador y el Centro Coordinador de Urgencias y Emergencias (CCUE).
- Registro automático de eventos, incluyendo mediciones, alarmas y descargas.

B. INTEGRACIÓN CON LA HISTORIA CLÍNICA DIGITAL EN MOVILIDAD (HCDM)

Integración obligatoria con la HCDM del SSPA

- El monitor deberá estar integrado o integrarse en un plazo máximo de 6 meses desde la adjudicación.
- Los costes de integración serán asumidos por el adjudicatario.

Requisitos técnicos de integración

El licitador deberá aportar:

- Librería SDK para intercambio de información con la HCDM

Es copia auténtica de documento electrónico

- Compatible con Windows
- Invocable desde proyectos .NET Framework 4.0 o superior
- Documentación técnica completa, incluyendo manual de uso y soporte técnico.

Estándares y seguridad

- La integración se realizará mediante HL7 o FHIR.
- La comunicación estará cifrada de extremo a extremo.
- El envío de datos será directo a la HCDM, sin intermediación de servidores externos del fabricante.
- La licencia del SDK será corporativa, sin restricciones de usuarios o dispositivos.

Visualización en tiempo real

Los parámetros, curvas y mediciones deberán transmitirse y visualizarse en tiempo real desde el monitor desfibrilador a la HCDM.

4. COMPOSICIÓN DEL SUMINISTRO

Los equipos se entregarán con todos los accesorios y fungibles listos para su uso y funcionalidad:

- Unidades de baterías para la configuración del equipo
- Una unidad de cable de derivaciones precordiales para ECG
- Una unidad de cable de monitorización de ritmo cardiaco
- Una unidad de cable de terapias eléctricas
- Una unidad de brazalete reutilizable adulto y pediátrico de PNI.
- Una unidad de electrodo multifunción (monitorización, DFV, marcapasos) pediátrico
- Una unidad de electrodo multifunción (monitorización, DFV, marcapasos) adulto
- Una unidad de sensor reutilizable para pulsioximetría adulto.
- Una unidad de sensor reutilizable para pulsioximetría pediátrico
- Una unidad de cable de capnografía
- Una unidad de accesorio para medición CPR
- Una unidad de soporte cargador 12V para ambulancia clase C.
- Una unidad de funda de transporte.
- Una unidad de cable carga a 220 V para baterías.

5. GARANTÍA Y SERVICIO POSTVENTA

El plazo de garantía mínimo de los bienes suministrados (equipos y accesorios) será de 2 años, contados a partir de la fecha de recepción definitiva con conformidad por parte del CES 061.

Durante dicho periodo, el contratista deberá garantizar, sin coste adicional para el CES 061, la prestación del servicio postventa, en los términos siguientes:

Es copia auténtica de documento electrónico

5.1. Sustitución temporal de equipos y accesorios averiados

En el caso de que la reparación de cualquier equipo o accesorio averiado se prevea que supere un plazo de siete (7) días naturales desde su entrega en el Servicio Técnico, el adjudicatario estará obligado a realizar la sustitución temporal por otro equipo de iguales características y configuración a los ofertados, en un plazo máximo de 48 horas o dos (2) días naturales.

5.2. Mantenimiento preventivo

Durante el periodo de garantía, el adjudicatario será responsable de realizar el mantenimiento preventivo prescrito por el fabricante, incluyendo, en su caso:

- Desplazamiento del personal técnico.
- Tiempo de mano de obra.
- Materiales consumibles.
- Baterías
- Piezas de recambio recomendadas en el manual de mantenimiento del fabricante (incluidas baterías).

Estas actuaciones deberán realizarse conforme al plan y periodicidad establecidos por el fabricante, sin coste adicional para la entidad contratante.

El licitador deberá detallar en su propuesta:

- El plan de mantenimiento preventivo propuesto.
- La frecuencia e intervenciones necesarias.
- La operativa prevista para su ejecución.

5.3. Actualizaciones y mejoras del equipo

El licitador de los monitores desfibriladores, durante el tiempo de garantía incluirá, sin coste adicional para el CES 061, las actualizaciones de software y/o firmware de los equipos ofertados.

5.4. Medios técnicos y gestión ante averías

El licitador deberá incorporar en su oferta técnica una descripción detallada de los recursos técnicos y humanos disponibles para la atención de incidencias, incluyendo al menos:

- Tiempos de respuesta garantizados.
- Número de personal técnico disponible y su cualificación.
- Ubicación del servicio técnico en España, y, delegaciones o puntos de asistencia cercanos a la comunidad autónoma andaluza.
- Canales de contacto directo (teléfono, correo).

Es copia auténtica de documento electrónico

6. CONDICIONES DE SUMINISTRO, PLAZO Y LUGAR DE RECEPCIÓN

La empresa adjudicataria deberá suministrar los equipos adjudicados, acompañados de todos los accesorios, consumibles y elementos necesarios para su uso completo y funcionamiento, de acuerdo con lo especificado en el apartado 4. Composición del Suministro.

Cada unidad deberá entregarse acompañada, en formato digital (PDF), de la siguiente documentación mínima:

- Manual de uso en castellano del equipo y sus accesorios.
- Manual técnico en castellano, con instrucciones de mantenimiento, configuración y resolución de incidencias.
- Certificado de Conformidad del Marcado CE para todos los elementos que lo requieran, conforme al Reglamento (UE) 2017/745.
- Programa de mantenimiento preventivo y técnico legal, especificando periodicidad, actuaciones requeridas y elementos críticos, conforme a las recomendaciones del fabricante.
- Cualquier otra documentación que facilite el conocimiento, manejo seguro, resolución de averías o incidencias, así como la trazabilidad del equipo.

6.1. Plazo de entrega y puesta en servicio

El plazo máximo de entrega de los equipos será de tres (3) semanas a contar desde la fecha de formalización del contrato.

La instalación, comprobación funcional y puesta en servicio de los equipos será realizada por el adjudicatario, en presencia del personal designado por CES 061. Al finalizar la instalación, se deberá emitir un informe de entrega y validación funcional conforme, firmado por ambas partes.

6.2. Lugar de entrega

La entrega y puesta en marcha de los equipos se realizará en la siguiente ubicación:

Sede Central del Centro de Emergencias Sanitarias 061

Parque Tecnológico de Andalucía

C/ Severo Ochoa, 28

29590 - Campanillas (Málaga)

7. FORMACIÓN

Con el fin de garantizar el uso seguro, eficaz y homogéneo de los equipos, la empresa adjudicataria deberá asumir la formación necesaria para la correcta capacitación en el manejo y mantenimiento de los referidos equipos suministrados. Esta formación se dirigirá a los profesionales sanitarios del CES 061 y se impartirá en un centro de la organización.

Monitores Desfibriladores

El programa formativo podrá desarrollarse mediante una de las siguientes metodologías, a elección del CES 061 en función de su planificación formativa:

- **Formación presencial**: realización de al menos dos sesiones prácticas presenciales durante una jornada de mañana en las instalaciones del CES 061, impartidas por personal cualificado

Es copia auténtica de documento electrónico

del adjudicatario.

- **Formación digital**: elaboración y entrega de videos tutoriales en castellano, que aborden los contenidos mínimos necesarios para el manejo, uso seguro, mantenimiento básico y resolución de incidencias del equipo.

La formación deberá impartirse tras la entrega de los equipos y podrá coordinarse con el personal del CES 061 conforme a las fechas que éste determine.

8. CIBERSEGURIDAD

El uso de tecnologías relacionadas con Internet of Medical Things (en adelante, IoMT) en entornos sanitarios ha crecido exponencialmente, aportando beneficios en la monitorización remota, el diagnóstico en tiempo real y la eficiencia clínica. Sin embargo, esta integración de dispositivos conectados implica también nuevos retos en materia de ciberseguridad, interoperabilidad, privacidad y continuidad asistencial, especialmente cuando dichos dispositivos manejan datos de carácter personal y clínico sensibles.

Las cláusulas recogidas en el Anexo II: Ciberseguridad se deben cumplir como medida para reforzar la seguridad de los entornos clínicos y fomentar una cultura de protección proactiva frente a amenazas que puedan comprometer la disponibilidad, integridad o confidencialidad de la información.

Es copia auténtica de documento electrónico

9. ANEXO I: Documentación a aportar –MONITORES DESFIBRILADORES

1. Documentación General y Administrativa

- Fichas técnicas oficiales: Correspondientes al modelo, versión y configuración ofertada.
- Declaración UE de conformidad: Emitida por el fabricante.

2. Normativa, Seguridad y Robustez (Certificados y Ensayos)

- Norma UNE-EN 1789 (Vehículos): Certificado o informe de ensayo acreditando que el equipo y su sistema de fijación cumplen requisitos de retención y resistencia a impactos.
- Norma IEC 60601-1 (Seguridad básica): Declaración del fabricante o certificado de ensayo del cumplimiento íntegro.
- Norma IEC 60601-1-2 (Compatibilidad electromagnética): Certificación de cumplimiento vigente.
- Norma IEC 60601-1-12 (Emergencias): Certificado oficial que acredite específicamente resistencia a vibración mecánica (aleatoria y sinusoidal), choque, caída libre y condiciones ambientales.
- Grado de protección IP55: Certificado de protección frente a polvo y agua.
- Rango de temperatura (0 a 45 °C): Certificado del fabricante que acredite este rango operativo para el equipo y su electrónica interna.

3. Características Físicas y Ergonomía

- Certificado de Peso: Documento emitido por el fabricante desglosando el peso del equipo sin funda, baterías, accesorios, funda y el peso total configurado (debe ser ≤ 9,5 kg).
- Dimensiones físicas: Aportar dimensiones (ancho x alto x fondo) en cm del equipo sin funda, verificables en la ficha técnica oficial.

4. Parámetros Clínicos y Funcionalidad

- Pantalla e Impresora: Ficha técnica con las especificaciones de estos componentes.
- Parámetros de monitorización: Documento certificado describiendo los parámetros (Rangos y características) de la versión ofertada.
- Tecnología en baja perfusión: Documentación técnica o certificación que acredite las prestaciones de SpO_2 y PANI en escenarios de baja perfusión.
- Ayuda a la RCP: Acreditación de que el equipo incluye sistema de calidad y ayuda a la RCP con sensor integrado o acelerómetro.
- Funciones avanzadas (Paciente crítico): Certificado o declaración del fabricante sobre la capacidad de predicción/detección temprana de deterioro, registro de tendencias y capacidad de ampliación funcional.

5. Alimentación y Soporte

- Autonomía: Documentación técnica que acredite valores de autonomía y capacidad de descarga.
- Soporte de ambulancia: Certificación oficial del fabricante o laboratorio acreditado del cumplimiento de normas del soporte.

Es copia auténtica de documento electrónico

6. Conectividad e Integración (HCDM)

- Conectividad inalámbrica: Indicación de los medios de conectividad para datos clínicos.
- Comunicación interna: Documentación técnica sobre el mecanismo de comunicación entre módulos.
- Kit de Integración (SDK):
    - Aportación de librería SDK compatible con Windows y .NET Framework 4.0 o superior.
    - Documentación técnica completa del SDK, incluyendo manual de uso y soporte.

7. Manuales, Mantenimiento y Servicio Técnico

- Manuales: Manual de uso y Manual técnico en castellano (formato digital PDF).
    - Instrucciones explícitas sobre la desfibrilación durante la compresión.
- Mantenimiento Preventivo:
    - Programa de mantenimiento preventivo y técnico legal que requieren los equipos.
    - Especificación de periodicidad de intervenciones y listado de piezas de recambio.
- Mantenimiento Correctivo y Soporte:
    - Descripción de recursos técnicos y humanos disponibles para la atención de incidencias.
    - Tiempos de respuesta garantizados.
    - Número de personal técnico disponible y su cualificación.
    - Ubicación del servicio técnico en España, detallando delegaciones o puntos de asistencia cercanos a la comunidad autónoma andaluza.
    - Canales de contacto directo (teléfono, correo).

10. Anexo II. Ciberseguridad

10.1. Gobernanza

10.1.1. Asignación de Responsabilidades

El adjudicatario será responsable de definir, documentar y mantener actualizada una matriz de roles y responsabilidades específica para la gestión de la seguridad de los dispositivos, sistemas y servicios relacionados con IoMT. Esta matriz deberá asignar claramente las funciones relacionadas el objeto del contrato, así como la gestión segura de dichos dispositivos. Además, deberá asignar un Punto Único de Contacto de Seguridad (POC), que actuará como interlocutor principal con la entidad sanitaria para todas las comunicaciones relativas a la seguridad de la información y la gestión de incidentes, dando soporte en el cumplimiento de los requisitos de ciberseguridad aplicables

Asimismo, cuando el adjudicatario asuma el mantenimiento y soporte de los entornos IoMT, deberá designar un responsable técnico por cada entorno, proporcionando al POC los recursos necesarios para coordinar las acciones de respuesta ante incidentes, manteniendo así la integridad, confidencialidad y disponibilidad de los datos médicos procesados por los dispositivos.

Es copia auténtica de documento electrónico

El adjudicatario garantizará que todos los roles asignados estén respaldados por la capacitación adecuada, documentación de procesos y mecanismos de supervisión periódica. Cualquier cambio en las responsabilidades deberá ser notificado y aprobado formalmente por la entidad contratante, asegurando una trazabilidad completa en la gestión de los activos IoMT.

10.1.2. Políticas y procedimientos

El adjudicatario deberá desarrollar, implementar y mantener Sistema de Gestión de Seguridad de la Información (SGSI), o un conjunto formal de políticas y procedimientos, con alcance específico en los dispositivos, sistemas y servicios relacionados con IoMT objeto del contrato. Dicho SGSI deberá estar alineado con los marcos regulatorios aplicables, las mejores prácticas de ciberseguridad y el cuerpo normativo de la entidad contratante.

Las políticas incluidas deberán abordar, aspectos como configuración inicial, control de acceso, monitorización continua, gestión de vulnerabilidades, aplicación de parches, desactivación segura y protección de datos personales y clínicos procesados por los dispositivos, sistemas y servicios relacionados con IoMT.

Los procedimientos asociados deberán ser detallados, operativos y actualizados regularmente, garantizando su alineación con las normativas de la entidad contratante.

Cualquier modificación en las políticas o procedimientos por parte del adjudicatario deberá ser debidamente registrada y aprobada por los órganos competentes del adjudicatario, comunicando a la entidad contratante aquellas variaciones que resulten relevantes para el objeto del contrato.

10.1.3. Gestión Documental

El adjudicatario será responsable de la elaboración, entrega y actualización de toda la documentación técnica y operativa relacionada con los dispositivos IoMT suministrados o gestionados en el marco del presente contrato. Dicha documentación deberá incluir manuales de usuario, guías de instalación, protocolos de mantenimiento, instrucciones de seguridad, y cualquier otro documento necesario para el correcto uso, gestión y soporte de los dispositivos por parte del personal sanitario y técnico.

Toda la documentación entregada a la entidad contratante deberá cumplir con los siguientes requisitos:

- Formato y lenguaje, la información deberá presentarse en un formato claro y estructurado, redactada preferiblemente en idioma español y utilizando un lenguaje técnico comprensible para profesionales sanitarios y técnicos. En los casos en que la documentación original solo esté disponible en inglés, deberá entregarse, como mínimo, en español toda la información necesaria para garantizar que los dispositivos se mantienen conforme a las recomendaciones del fabricante, especialmente en lo relativo a la seguridad y a la conservación de las condiciones durante su vida útil.
- Accesibilidad, el adjudicatario deberá garantizar que toda la documentación pueda ser almacenada en el repositorio centralizado de la entidad contratante, siguiendo los procedimientos y formatos establecidos por esta, de forma que se asegure su correcta integración y disponibilidad para su posterior consulta por parte del personal autorizado.
- Actualización continua, la documentación deberá actualizarse durante toda la vigencia del contrato, incorporando cualquier cambio en configuraciones, versiones de software, funcionalidades o normativas aplicables.

Es copia auténtica de documento electrónico

10.2. Cumplimiento normativo

10.2.1. Normativa y conformidad

El adjudicatario será responsable de garantizar que todos los dispositivos, sistemas y servicios relacionados con IoMT suministrados o gestionados en el marco del presente contrato se encuentren plenamente adecuados a la normativa vigente en materia de ciberseguridad aplicable al sector sanitario.

En el caso de dispositivos médicos IoMT, deberá acreditar que cuentan con marcado CE y que cumplen los requisitos establecidos en el Reglamento (UE) 2017/745 (MDR) o el Reglamento (UE) 2017/746 (IVDR), según corresponda.

Asimismo, para el resto de los dispositivos y servicios asociados, el adjudicatario deberá aportar, evidencias verificables que acrediten el cumplimiento de las obligaciones contractuales y normativas, como ENS, RGPD y LOPDGDD, mediante certificaciones vigentes, informes de auditoría externa, pruebas de conformidad realizadas por terceros cualificados o, en su defecto, documentación técnica que demuestre la correcta aplicación de las medidas exigidas.

Por otro lado, deberá exigir a los técnicos que formen parte del equipo de trabajo objeto de este contrato el cumplimiento de la normativa de seguridad establecida por la entidad sanitaria en relación con las obligaciones y funciones del personal. El adjudicatario quedará obligado frente a la entidad por las responsabilidades que puedan derivarse del incumplimiento de esta normativa.

10.3. Gestión de accesos y usuarios

10.3.1. Sistemas de Control de Acceso y Autenticación

Los dispositivos, sistemas y servicios relacionados con IoMT deberán disponer de un sistema de control de acceso robusto que garantice que únicamente el personal debidamente autorizado pueda acceder a los datos personales tanto del personal interno como de los pacientes.

En caso de que el dispositivo o sistema lo permita, se deberán implementar controles de acceso basados en roles RBAC (del inglés, Role Based Access Control) de manera que las aplicaciones permitan el establecimiento de distintos grupos de usuarios en función de las actividades que realicen. Dichos grupos deberán estar identificados y detallados en base a los privilegios de los mismos y sus responsabilidades asociadas.

El adjudicatario tiene la obligación de establecer procedimientos internos formales para notificar oportunamente a la entidad contratante la necesidad de cualquier alta, modificación y/o baja de los usuarios prestadores de los servicios, garantizando que la entidad lleve a cabo el bloqueo y posterior eliminación de las cuentas asociadas.

10.3.2. Procedimientos de Autorización de Acceso

Los mecanismos de control de acceso deberán estar alineados con los procedimientos establecidos por la entidad contratante para las autorizaciones de acceso a los dispositivos y sus sistemas de información relacionados.

Las políticas de acceso y autorización serán revisadas y actualizadas periódicamente por el adjudicatario para reflejar posibles cambios en el personal y las necesidades de seguridad, garantizando que solo el personal necesario tenga acceso a información sensible.

La entidad contratante podrá llevar a cabo auditorías regulares para asegurar el cumplimiento de los

Es copia auténtica de documento electrónico

procedimientos de autorización de acceso y para identificar y corregir cualquier desviación.

10.4. Gestión del acceso remoto para servicios de mantenimiento

10.4.1. Autorización Previa para Herramientas de Acceso Remoto

El adjudicatario no podrá instalar ni utilizar herramientas o mecanismos de acceso remoto a los dispositivos, sistemas o plataformas vinculadas a soluciones IoMT sin la autorización previa, expresa y por escrito de la entidad contratante.

La autorización deberá solicitarse para cada herramienta específica, detallando su finalidad, alcance técnico, medidas de seguridad implementadas, trazabilidad de las acciones realizadas y el personal autorizado para su uso.

Ninguna herramienta de acceso remoto destinada a la prestación de servicios de mantenimiento o resolución de incidencias en dispositivos médicos y sus sistemas de información relacionados se considerará preautorizada sin la aprobación explícita de la entidad contratante.

10.4.2. Uso de Servicios VPN

El adjudicatario deberá utilizar preferentemente los servicios corporativos de Red Privada Virtual (en adelante, VPN) sede a sede proporcionados por la entidad contratante.

En caso de requerirse una solución de VPN distinta, esta deberá contar con la autorización previa, expresa y por escrito de la entidad antes de su uso.

Las soluciones empleadas deberán garantizar la confidencialidad, integridad y autenticación de las comunicaciones, así como cumplir con los requisitos técnicos y normativos aplicables en materia de seguridad y operatividad para el ámbito sanitario.

Todas las comunicaciones realizadas a través de la VPN deberán estar cifradas y autenticadas adecuadamente, empleando mecanismos de cifrado robustos y estándares actualizados.

La arquitectura y configuración de la VPN utilizada deberá alinearse con los principios del Esquema Nacional de Seguridad (ENS) o encontrarse incluida en el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información (CPSTIC) del CCN-CERT, siendo asimismo valorable su conformidad con estándares de seguridad reconocidos como ISO/IEC 27001 o equivalentes.

El adjudicatario será responsable de proporcionar la documentación técnica de la solución VPN propuesta, así como de garantizar su correcta operación, mantenimiento y actualización.

Queda expresamente prohibido el uso de soluciones de conectividad no autorizadas, genéricas o de carácter comercial no controlado.

10.4.3. Autenticación Multifactor

Es obligatorio el uso de autenticación multifactor (en adelante, MFA) para todos los accesos remotos a los dispositivos médicos, sus sistemas de información y los servicios relacionados con IoMT por parte del adjudicatario.

Los mecanismos de MFA implementados deberán ser avanzados y garantizar la verificación robusta de la identidad de los usuarios que acceden a los sistemas, asegurando la confidencialidad e integridad de la conexión.

Es copia auténtica de documento electrónico

En caso de que el adjudicatario proporcione sus propias herramientas de acceso remoto, será responsable de su correcta configuración, mantenimiento y actualización, así como de registrar y conservar los logs de acceso de forma trazable y auditable.

No se permitirá el uso de credenciales compartidas ni de mecanismos de autenticación que no cumplan con los niveles de seguridad exigidos por la entidad contratante y la normativa aplicable.

10.4.4. Autorización de Usuarios

Solo los usuarios previamente autorizados por la entidad contratante a propuesta del adjudicatario tendrán los derechos de acceso necesarios para la prestación de servicios de mantenimiento y resolución de incidencias mediante acceso remoto a los dispositivos, sistemas y servicios relacionados con IoMT.

El adjudicatario será responsable de la gestión de la identidad de los profesionales que presten los servicios, garantizando en todo momento que únicamente dispongan de los permisos estrictamente necesarios y que estos se actualicen de acuerdo con las altas y bajas en el equipo de trabajo.

10.4.5. Propuesta de Herramientas de Acceso Remoto para el Adjudicatario

El adjudicatario podrá proponer herramientas específicas de acceso remoto dispositivos, sistemas y servicios relacionados con IoMT para la prestación de servicios de mantenimiento y resolución de incidencias.

Las soluciones de acceso remoto deberán respetar la arquitectura de seguridad de la entidad contratante, incluyendo la arquitectura de protección de perímetro tipo 6 (APP-6) según lo establecido en la Guía de Seguridad TIC CCN-STIC 811.

10.4.6. Evaluación Excepcional de Herramientas de Acceso Remoto

En casos donde la herramienta propuesta por el adjudicatario no soporte la arquitectura de seguridad APP-6 o no pueda utilizar servicios de VPN, la entidad contratante podrá evaluar excepcionalmente el uso de otras herramientas propuestas por el adjudicatario.

Asimismo, en caso de que dichas herramientas no resulten adecuadas, podrá considerarse la prestación de los servicios de forma presencial en las instalaciones de la entidad contratante, respetando en todo momento la normativa relativa al control de acceso físico.

Las herramientas podrán ser autorizadas si cumplen con las condiciones de seguridad necesarias y no incrementan el riesgo para la seguridad de las infraestructuras de la entidad contratante.

Corresponderá al adjudicatario demostrar el cumplimiento de las condiciones de seguridad necesarias mediante análisis y pruebas de seguridad realizadas por terceros independientes acreditados.

El adjudicatario será responsable de que las herramientas propuestas no presenten vulnerabilidades conocidas en el momento de su puesta en servicio, así como, garantizar su actualización y mantenimiento durante toda la prestación, incorporando su gestión al circuito de incidencias y, en su caso, bloqueando de forma inmediata el acceso cuando resulte necesario.

Es copia auténtica de documento electrónico

10.5. Gestión de activos OT

10.5.1. Clasificación de Activos OT

El adjudicatario deberá entregar, junto con cada dispositivo, sistema o servicio IoMT, la información necesaria para su correcta clasificación según criterios de criticidad clínica, nivel de exposición a amenazas, grado de conectividad y cualquier otro dato relevante que facilite la evaluación de riesgos.

La integración de esta información en los sistemas internos de gestión de riesgos será responsabilidad exclusiva de la entidad contratante.

10.5.2. Inventario de Activos

El adjudicatario deberá proporcionar, en el momento de la entrega, los datos técnicos necesarios para que la entidad contratante incorpore los dispositivos y sistemas IoMT a su inventario corporativo, incluyendo aspecto como modelo, versión de firmware, fabricante, ubicación física, número de serie y estado operativo.

Cuando el adjudicatario sea además fabricante, deberá mantener su propio inventario interno de los equipos que suministra, asignando un responsable técnico y registrando toda información relevante para su trazabilidad y gestión.

10.5.3. Control de Alta, Baja y Modificación de Activos

El adjudicatario deberá implementar un procedimiento formal y documentado para registrar, comunicar y respaldar cualquier alta, modificación, traslado o baja de los activos IoMT relacionados con los servicios prestados en el marco del presente contrato, incluyendo cambios derivados del mantenimiento, actualización, deterioro, sustitución o reubicación de los dispositivos y sistemas.

Dicho procedimiento deberá garantizar el registro detallado de cada operación, incluyendo fecha, responsable y descripción técnica del cambio, así como la comunicación a la entidad en caso de que resulte necesario.

Además, deberá aportar la documentación y datos técnicos necesarios para mantener la trazabilidad completa de los dispositivos y sistemas, así como de los datos tratados por los mismos, asegurando que toda actuación quede adecuadamente registrada y reportada a la entidad contratante.

10.6. Configuración segura

10.6.1. Configuración Inicial Segura

El adjudicatario garantizará que, en el momento de la entrega y despliegue de los dispositivos, sistemas y servicios relacionados con IoMT en los centros sanitarios, sean configurados siguiendo los parámetros de configuración segura definidos por el fabricante y alineados con las buenas prácticas de ciberseguridad, evitando así el uso de configuraciones predeterminadas inseguras.

Paralelamente, todas las credenciales predeterminadas por el fabricante serán cambiadas inmediatamente después de la instalación del dispositivo y antes de su primer uso, garantizando así que no se utilicen credenciales de fábrica.

10.6.2. Deshabilitación de Servicios

El adjudicatario deshabilitará todos los servicios y puertos no necesarios en los dispositivos, sistemas y servicios relacionados con IoMT para minimizar la superficie de ataque, asegurando que solo permanezcan funcionales los estrictamente necesarios para el funcionamiento del dispositivo.

Es copia auténtica de documento electrónico

10.7. Actualizaciones de software

10.7.1. Políticas de Actualización

El adjudicatario deberá establecer y mantener políticas claras y documentadas para la actualización de hardware y software de los dispositivos médicos, garantizando que todos los dispositivos estén equipados con los últimos parches de seguridad y firmware antes de ser puestos en producción.

Se implementará un proceso regular y sistemático de actualización y parcheo para mantener los dispositivos, sistemas y servicios relacionados con IoMT.

Todas las actualizaciones realizadas se harán empleando fuentes y librerías oficiales del fabricante o recomendadas por este.

10.7.2. Actualizaciones Automáticas

Siempre que sea posible y no represente un riesgo para el funcionamiento o el rendimiento de los dispositivos, sistemas y servicios relacionados con IoMT, el adjudicatario habilitará procesos de actualización automáticos.

Estos procesos permitirán que los dispositivos se actualicen automáticamente para aplicar parches de seguridad y mejoras.

El adjudicatario garantizará que las actualizaciones automáticas sean configurables permitiendo definir horarios de actualización y así minimizar interrupciones en la operativa sanitaria.

10.7.3. Mecanismos Seguros de Actualización

El adjudicatario deberá implementar mecanismos seguros para la actualización de software, asegurando la autenticidad e integridad de las actualizaciones mediante un plan periódico.

Asimismo, el adjudicatario deberá asegurar la disponibilidad de mecanismos de reversión segura (del inglés, rollback) que permitan restaurar la configuración o versión anterior del sistema o dispositivo en caso de fallo, incompatibilidad, impacto clínico o degradación del servicio tras la actualización.

El procedimiento de rollback deberá estar documentado, probado y ser ejecutable sin comprometer la integridad de los datos ni la continuidad asistencial.

10.7.4. Evaluación de Impacto y Pruebas

El adjudicatario llevará a cabo, en sus instalaciones, evaluaciones de impacto exhaustivas con el objetivo de evaluar el efecto de las actualizaciones en el funcionamiento de los dispositivos, sistemas y servicios relacionados con IoMT y la seguridad del paciente antes de su implementación.

Todos los parches y actualizaciones serán revisados y probados en un entorno de pruebas controlado ubicado en las instalaciones del adjudicatario, siguiendo procedimientos estandarizados que permitan minimizar los riesgos de interrupciones y garantizar la resiliencia de los sistemas antes de su despliegue en los entornos de la entidad contratante.

10.7.5. Documentación y Notificación

El adjudicatario mantendrá una gestión documental para el seguimiento y registro de todas las actualizaciones aplicadas, incluyendo la fecha, el contenido de las actualizaciones y los dispositivos, sistemas y servicios relacionados con IoMT.

Se notificará e informará al personal TI responsable asignado por la entidad contratante, así como al personal técnico correspondiente cuando sea necesario, acerca de las actualizaciones realizadas y de

Es copia auténtica de documento electrónico

cualquier cambio previsto en el funcionamiento de los dispositivos.

10.8. Gestión de vulnerabilidades

10.8.1. Proceso de Identificación y Gestión de Vulnerabilidades

El adjudicatario deberá implementar y mantener un proceso continuo y proactivo para la identificación y gestión de vulnerabilidades en sus entornos, a lo largo del ciclo de vida de todos los dispositivos, sistemas y servicios relacionados con IoMT que se encuentren bajo su responsabilidad, durante toda la vigencia del contrato.

Este proceso deberá incluir la consulta periódica de bases de datos públicas de vulnerabilidades reconocidas internacionalmente, así como la utilización de fuentes de inteligencia de amenazas, tales como informes especializados de ciberseguridad y repositorios de vulnerabilidades.

10.8.2. Análisis Regular de Vulnerabilidades

El adjudicatario realizará análisis de vulnerabilidades periódicos en los dispositivos, sistemas y servicios relacionados con IoMT objeto del contrato, utilizando herramientas avanzadas de escaneo y pruebas de penetración.

Dichos análisis deberán llevarse a cabo exclusivamente en las instalaciones del adjudicatario, siendo responsabilidad de la entidad contratante la monitorización y gestión de las vulnerabilidades de los dispositivos y sistemas desplegados en sus entornos.

El adjudicatario documentará de manera exhaustiva las vulnerabilidades, tanto las ya identificadas como las potenciales, asociadas a cada dispositivo, asegurando una transparencia total durante el proceso de resolución.

10.8.3. Notificación y Plan de Corrección

El adjudicatario notificará regularmente a la entidad contratante los resultados de los análisis de vulnerabilidades llevados a cabo en sus instalaciones, proponiendo además un plan de corrección y priorización de las debilidades en los dispositivos, sistemas y servicios relacionados con IoMT analizados, con la finalidad de ser aplicadas medidas correctoras sobre los activos desplegados en las instalaciones de la entidad contratante.

10.8.4. Implantación inicial libre de vulnerabilidades

Los dispositivos médicos adquiridos deberán estar libres de vulnerabilidades conocidas en el momento de la instalación en los centros sanitarios.

En caso de que, por razones técnicas o legales, no sea posible un despliegue inicial completamente libre de vulnerabilidades conocidas, el adjudicatario deberá proporcionar a la entidad contratante el último informe de análisis de vulnerabilidades disponible.

Dicho informe deberá identificar las vulnerabilidades conocidas hasta la fecha, evaluar el nivel de riesgo asociado a cada una y presentar un plan de corrección y priorización que contemple los plazos estimados para su resolución.

Asimismo, el adjudicatario deberá proponer e implementar las medidas de seguridad compensatorias necesarias para reducir la probabilidad de explotación de las vulnerabilidades no corregidas, de forma que el riesgo residual se mantenga por debajo del umbral de riesgo aceptable definido por la entidad contratante.

Es copia auténtica de documento electrónico

10.9. Desarrollo seguro

10.9.1. Seguridad desde el diseño

El adjudicatario deberá garantizar que todos los dispositivos médicos IoMT, así como el software incorporado o considerado dispositivo médico suministrado en el marco del presente contrato, cuenten, en el momento de su entrega, con:

Marcado CE válido, colocado en el dispositivo, así como la documentación asociada que acredite que el producto cumple con los requisitos relativos a seguridad desde el diseño y seguridad por defecto establecidos en el Reglamento (UE) 2017/745 (MDR) o el Reglamento (UE) 2017/746 (IVDR).

Declaración UE de Conformidad, expedida por el fabricante, en la que se declare bajo su responsabilidad que el dispositivo cumple con todos los requisitos aplicables establecidos en la normativa europea vigente. Esta declaración deberá estar disponible para la entidad contratante.

Documentación técnica actualizada, emitida por el fabricante, que permita verificar el cumplimiento de los requisitos de seguridad, interoperabilidad y ciberseguridad, incluyendo las especificaciones aplicables para su integración en el entorno operativo de la entidad contratante.

Sin la presentación y validación previa de estas certificaciones y documentos, el dispositivo no podrá ser aceptado ni autorizado para su puesta en producción en los entornos de la entidad contratante.

Además, los dispositivos, sistemas y servicios que, sin ser considerados dispositivos médicos, estén incluidos en el alcance del presente contrato deberán estar diseñados para minimizar los riesgos desde su concepción.

Para ello deberán incorporar medidas técnicas como control de accesos, autenticación robusta, cifrado de datos en tránsito y en reposo, protección frente a código malicioso, registros de auditoría y separación de funciones críticas, cumpliendo así con los requisitos aplicables del Esquema Nacional de Seguridad (ENS).

10.10. Mantenimiento físico de los dispositivos

10.10.1. Coordinación con el equipo técnico y clínico

El adjudicatario deberá establecer mecanismos de coordinación efectiva, continua y documentada con los equipos técnicos y clínicos de la entidad contratante para todas las actividades relacionadas con la instalación, configuración, integración, mantenimiento y actualización de los dispositivos, sistemas y servicios relacionados con IoMT.

Esta coordinación será esencial para garantizar la seguridad del paciente, la interoperabilidad con los sistemas asistenciales y la operatividad de los servicios clínicos.

También, el adjudicatario deberá designar interlocutores técnicos cualificados que actúen como puntos de contacto con las áreas de ingeniería clínica, tecnologías de la información y los servicios asistenciales, así como facilitar la planificación conjunta de intervenciones, validaciones funcionales y pruebas de integración.

Toda acción que pueda afectar el funcionamiento de los dispositivos médicos conectados o la disponibilidad de servicios clínicos deberá ser previamente comunicada, acordada y autorizada por la entidad contratante.

Es copia auténtica de documento electrónico

10.11. Acceso de emergencia autorizado al dispositivo

10.11.1. Mecanismo de Acceso de Emergencia

El adjudicatario deberá implementar en los dispositivos, sistemas y servicios relacionados con IoMT un mecanismo de acceso de emergencia que permita a usuarios autorizados acceder temporalmente a funciones críticas del dispositivo en situaciones clínicas urgentes, cuando los controles de acceso estándar puedan causar demoras perjudiciales para el paciente.

El adjudicatario deberá asegurar que el acceso de emergencia solo pueda ser realizado por personal de que esté previamente autorizado por la entidad contratante, técnicamente limitado en su alcance, registrado de forma completa y trazable, y sujeto a revisión posterior.

Los mecanismos de acceso de emergencia deben activarse solo bajo condiciones justificadas y conforme a políticas predefinidas, garantizando en todo momento la integridad del sistema y la confidencialidad de los datos.

10.12. Seguridad contra el código dañino

10.12.1. Uso de software de protección contra código dañino

Se utilizará software de protección frente a código dañino que pudiera comprometer el uso de los dispositivos por parte de actores de amenazas.

En aquellos casos en que las especificaciones del fabricante del dispositivo o de sus sistemas relacionados no lo permitan, deberán aplicarse las medidas compensatorias correspondientes.

Tendrán siempre preferencia los sistemas de protección contra código dañino propios de la entidad contratante, ya que sus alertas son monitorizadas y supervisadas por la propia entidad y/o sus CERT de referencia.

En aquellos casos en los que el fabricante del dispositivo imponga una determinada herramienta para la protección contra código dañino, el adjudicatario deberá especificar quién o qué organismo o empresa y de qué forma se monitorizan las alertas ocurridas en los dispositivos objeto de adjudicación, así como de qué forma se comunicarán estas al CERT de referencia de la entidad contratante.

Asimismo, el adjudicatario deberá asegurarse de que el fabricante entregue un manual de seguridad que incluya los requisitos mínimos del dispositivo en materia de seguridad, incorporando, entre otros, aspectos como segmentación, cifrado, mecanismos de registro, copias de seguridad y cualquier requisito adicional necesario para ser evaluado por la entidad contratante.

Los productos o servicios de seguridad propuestos por el fabricante deberán figurar en el CPSTIC del CCN-CERT, o, en su defecto, contar con certificaciones equivalentes que acrediten la funcionalidad de seguridad requerida, como el cumplimiento de lo establecido en el artículo 19 del Esquema Nacional de Seguridad (ENS) en caso de la prestación de servicios.

Asimismo, para todos los productos o servicios propuestos, el tiempo de comunicación de alertas será siempre inmediato, es decir, en tiempo real.

En todo caso, si el sistema relacionado con el dispositivo presta un servicio web, este deberá ser protegido frente a ataques de manipulación, inyección de código e inyección SQL al menos mediante validación y saneamiento de entradas, uso de funciones seguras, control de accesos y privilegios, filtros y escapes de caracteres especiales, manejo adecuado de errores, etc.

Adicionalmente, la monitorización de la seguridad de los dispositivos en los entornos de la entidad

Es copia auténtica de documento electrónico

contratante será responsabilidad exclusiva de esta, siguiendo sus propias políticas y procedimientos.

El adjudicatario únicamente deberá garantizar que, en el manual de seguridad, se incluyan los mecanismos y recomendaciones de seguridad proporcionados por el fabricante para su correcta integración y gestión.

10.13. Capacidad de bloqueo del dispositivo

10.13.1. Niveles de Bloqueo Configurables

Los dispositivos IoMT implementados por parte del adjudicatario deberán permitir la configuración de múltiples niveles de bloqueo según el contexto clínico, técnico o administrativo definido por la entidad contratante:

- Bloqueo total (inhabilitación completa del dispositivo).

- Bloqueo funcional (inhabilitación de funciones específicas).

- Bloqueo temporal (suspensión programada o automatizada), según el contexto clínico, técnico o administrativo definido por la entidad contratante.

O en caso de servicio de urgencias o dispositivos críticos clase III (MDR), no estará permitido el bloqueo del dispositivo (Perfil de Cumplimiento Especifico CCN-STIC 891).

10.14. Gestión de eventos

10.14.1. Registros de Seguridad y Configuración de Logs

Los dispositivos médicos deberán permitir la activación y configuración de registros de seguridad de manera detallada y continua para el análisis y trazabilidad de eventos.

El adjudicatario deberá disponer de mecanismos adecuados de recepción, gestión y seguimiento de incidencias, como sistemas de ticketing o equivalentes, que le permitan recibir, evaluar y atender de forma diligente cualquier evento que le sea notificado por la entidad contratante, ya sea derivado de la detección de vulnerabilidades, errores operativos o la sospecha de incidentes de seguridad.

La configuración de los dispositivos, sistemas y servicios relacionados con IoMT debe permitir establecer políticas de retención de logs adecuadas para asegurar que los registros estén disponibles en caso de auditoría durante un período determinado, de acuerdo con las mejores prácticas y regulaciones aplicables.

Los registros deberán almacenarse en formatos estructurados y estandarizados, preferentemente XML, JSON o Syslog, que permitan su integración automatizada con herramientas de análisis, sistemas de monitorización clínica o plataformas de seguridad (como SIEM o CMDB).

Los formatos seleccionados deberán garantizar la interoperabilidad, la legibilidad técnica y la integridad de los datos registrados.

Asimismo, deberá contemplarse la existencia de un perfil de auditor con permisos únicamente de lectura, que pueda acceder y visualizar los logs en caso de incidente, garantizando la trazabilidad y el análisis forense sin comprometer la integridad de la información.

10.14.2. Monitorización Continua y Revisión de Auditoría

Los entornos IoMT deberán permitir la monitorización continua mediante sistemas automatizados desplegados por la entidad contratante para la detección de intrusiones, accesos no autorizados,

Es copia auténtica de documento electrónico

actividades sospechosas o no autorizadas.

Los dispositivos médicos y sus sistemas de información relacionados dispondrán de la capacidad necesaria para que la entidad contratante pueda llevar a cabo revisiones periódicas de los registros de auditoría para identificar cualquier acceso no autorizado o actividad sospechosa.

10.15. Gestión de incidentes

10.15.1. Proceso Integral de Gestión de Incidentes

El adjudicatario dispondrá de un procedimiento integral para hacer frente a los incidentes ocurridos en sus instalaciones que puedan tener impacto en la seguridad de los sistemas o servicios que presta a la entidad contratante.

Este proceso incluirá procedimientos claros y detallados para la detección, análisis, contención, erradicación y recuperación de incidentes de seguridad.

Paralelamente, el adjudicatario asignará roles y responsabilidades específicas a miembros del equipo técnico de cara a garantizar una gestión eficaz de los incidentes, incluyendo la capacidad de asignar recursos para detectar, contener, erradicar, recuperar y analizar las consecuencias del incidente (lecciones aprendidas).

El adjudicatario deberá implementar procedimientos formalmente documentados que aseguren la recogida, conservación, transporte, acceso y análisis de evidencias digitales (como imágenes de memoria o disco, registros de acceso, trazas de actividad del sistema, etc.), aplicando técnicas que preserven su autenticidad, integridad y trazabilidad.

10.15.2. Procedimientos de Contención y Recuperación

El adjudicatario implementará procedimientos de contención con la mayor eficacia posible, limitando el alcance y el impacto de los incidentes de seguridad ocurridos en sus instalaciones que puedan afectar a los dispositivos, sistemas y servicios relacionados IoMT objeto del contrato.

10.15.3. Notificación de Incidentes

El adjudicatario notificará, con carácter inmediato, a los responsables de la entidad contratante y a las autoridades competentes sobre los incidentes de seguridad ocurridos en sus instalaciones, según lo requieran las normativas aplicables y cuando el incidente pudiera afectar a los servicios prestados por el adjudicatario a la entidad o este pudiera repercutir de alguna forma en sus dispositivos, sistemas y servicios relacionados con IoMT.

Asimismo, el adjudicatario informará de las actuaciones llevadas a cabo para la resolución del incidente y su impacto en la operativa.

Se definirán claramente las cadenas de mando y las responsabilidades de comunicación de forma proactiva antes de que se produzcan incidentes, a fin de asegurar una respuesta coordinada y eficiente entre el adjudicatario y la entidad contratante, de acuerdo con los procedimientos internos de gestión de incidentes establecidos.

10.15.4. Canales de Comunicación para Incidentes

Para una comunicación ágil de los incidentes, el adjudicatario deberá emplear los canales de comunicación establecidos por la entidad contratante, asegurando que la información llegue a todos los involucrados.

Es copia auténtica de documento electrónico

El adjudicatario utilizará estos canales para el reporte y seguimiento de incidentes de seguridad mediante los protocolos de comunicación definidos, garantizando que todas las partes interesadas sean informadas adecuadamente durante un incidente.

Esto incluirá la comunicación con el personal interno de la entidad contratante, otros proveedores, autoridades y pacientes, en su caso.

10.16. Gestión segura de la cadena de suministro

10.16.1. Evaluación de Terceros Proveedores relacionados con la adjudicación

El adjudicatario dispondrá de mecanismos y criterios de seguridad rigurosos para la evaluación y selección de sus propios proveedores que tengan relación con la relación contractual.

Dichos criterios deben incluir la revisión de las políticas de seguridad, prácticas de manejo de datos, y medidas de ciberseguridad implementadas por los proveedores.

El adjudicatario dispondrá de la capacidad para llevar a cabo auditorías periódicas de seguridad de sus proveedores para asegurar que cumplen con los requisitos de seguridad establecidos.

Las auditorías deben incluir evaluaciones de vulnerabilidades, revisiones de cumplimiento normativo y pruebas de penetración.

En su defecto podrán exigir las certificaciones de seguridad equivalentes de acuerdo con la normativa aplicable.

10.16.2. Contratos y Acuerdos

El adjudicatario incluirá cláusulas de seguridad específicas en todos los contratos y acuerdos con sus proveedores relacionados con esta adjudicación.

Estas cláusulas deben cubrir aspectos como la protección de datos, la respuesta a incidentes, la gestión de acceso y la obligación de mantener actualizadas las medidas de seguridad.

Estos contratos se revisarán periódicamente para asegurar que las cláusulas de seguridad sigan siendo relevantes y efectivas.

Las revisiones deben tener en cuenta cambios en las normativas, avances tecnológicos y lecciones aprendidas de incidentes de seguridad pasados.

Es de mencionar, que todas las cláusulas de seguridad de la información y ciberseguridad desarrolladas en el presente pliego, en el caso de disponer de terceros que realicen alguna operación sobre los dispositivos, sistemas y servicios relacionados con IoMT serán de aplicación directa, siendo el adjudicatario responsable de su traslado y cumplimiento.

10.17. Gestión de la obsolescencia

10.17.1. Planificación de la Restitución y Transferencia Tecnológica

El adjudicatario presentará una planificación detallada para la restitución y transferencia tecnológica, contemplando medios, acciones de contingencia y riesgos potenciales.

Cuando sea necesario, se incluirá un período de transición para la gestión organizada del proceso de transferencia.

En este sentido, el adjudicatario elaborará un plan detallado de transición que incluya todas las etapas

Es copia auténtica de documento electrónico

del proceso, asegurando la coordinación efectiva entre todas las partes involucradas.

10.18. Protección de los servicios Cloud

10.18.1. Localización y Ubicación Geográfica de los Datos Personales

El adjudicatario deberá informar a la entidad contratante sobre la ubicación geográfica de los datos, incluidas copias de seguridad y almacenamiento de logs, antes y durante el suministro del servicio.

Si los dispositivos médicos o sus sistemas relacionados manejan datos personales ubicados en la nube, se deberá asegurar en todo momento que la localización de los servidores donde se almacenan estos datos se encuentre en territorio de la Unión Europea, o, en su caso, en países o entidades que ofrezcan garantías adecuadas conforme al RGPD, mediante decisiones de adecuación la Comisión Europea o la aplicación de cláusulas contractuales.

Asimismo, cualquier cambio de ubicación deberá de ser notificado y aprobado por la entidad contratante.

Con respecto a los datos almacenados, se deberá cumplir con la Ley 3/2018 LOPDGDD y el resto de las normativas relacionadas en materia de protección de datos, junto a los perfiles de cumplimiento en ciberseguridad establecidos por el ENS (CCN-STIC 823) y estándares, como la ISO 27001 e ISO 27017.

El adjudicatario deberá colaborar en todo momento con el responsable del tratamiento designado por la entidad contratante de cara a garantizar el ejercicio de los derechos de protección de datos conforme a las normativas aplicables.

10.19. Continuidad de negocio

10.19.1. Procedimientos de Respaldo y Recuperación

El adjudicatario deberá proporcionar, junto con la documentación técnica de los dispositivos, sistemas y servicios IoMT, los procedimientos recomendados para la realización de copias de seguridad, restauración controlada y recuperación de la información almacenada o gestionada por los equipos suministrados.

Estos procedimientos deberán incluir como mínimo:

- Recomendaciones sobre la periodicidad de las copias de seguridad.

- Procedimientos de restauración verificados y probados sobre los dispositivos.

- Recomendaciones sobre cifrado y almacenamiento seguro de la información crítica.

10.19.2. Plan de Recuperación ante Contingencias

El adjudicatario deberá aportar la información técnica necesaria para que la entidad contratante pueda incluir los dispositivos y sistemas IoMT en su plan de recuperación ante contingencias.

En ningún caso el adjudicatario será responsable de ejecutar o coordinar dicho plan sobre la infraestructura de la entidad contratante.

En los casos en que el contrato incluya servicios gestionados relacionados con IoMT, los niveles de servicio, tiempos máximos de respuesta y procedimientos de recuperación estarán definidos mediante los Acuerdos de Nivel de Servicio (ANS) acordados entre las partes.

Es copia auténtica de documento electrónico

10.20. Auditorías técnicas y de cumplimiento

10.20.1. Requisitos de Pruebas de Seguridad

El adjudicatario deberá garantizar la realización de pruebas de seguridad sistemáticas y documentadas sobre todos los dispositivos, sistemas y servicios relacionados con IoMT previas a su puesta en producción, con el fin de identificar vulnerabilidades técnicas, errores de configuración, riesgos de exposición de datos y posibles vectores de ataque que puedan comprometer la confidencialidad, integridad, disponibilidad o trazabilidad de la información y de la operativa clínica.

Las pruebas deberán realizarse en coordinación con el órgano responsable de ciberseguridad de la entidad contratante, que tendrá la autoridad para suspender temporalmente el despliegue en caso de detectarse vulnerabilidades que puedan comprometer la seguridad de la entidad.

10.20.2. Capacidad para Pruebas de Seguridad y Auditorías

Los dispositivos, sistemas y servicios relacionados con IoMT adquiridos deberán tener la capacidad de ser sometidos a pruebas de seguridad y auditorías que verifiquen al menos los siguientes aspectos:

Auditorías de seguridad sobre el registro de actividades de los dispositivos médicos y los sistemas de información relacionados.

Revisiones de auditoría para identificar accesos no autorizados o actividades sospechosas, incluyendo la monitorización en tiempo real mediante herramientas automatizadas y el envío de telemetría a herramientas de correlación de datos.

Revisión y evaluación del cumplimiento y la efectividad de las políticas de seguridad de la entidad contratante, incluyendo la necesidad de ajustes según sea necesario.

Revisión y evaluación del cumplimiento normativo para asegurar el alineamiento con normativas y estándares relevantes.

Evaluación de los controles técnicos y los procedimientos de seguridad del proveedor.

El adjudicatario deberá colaborar, cuando sea requerido, con la entidad contratante en la realización de auditorías y pruebas de seguridad periódicas sobre los dispositivos, sistemas y servicios relacionados con IoMT, ya sea tras cambios significativos en los mismos o ante la sospecha de incidentes de seguridad.

Esta colaboración tiene por objeto asegurar el cumplimiento de las políticas de seguridad, facilitar la detección de vulnerabilidades y posibles brechas, y contribuir a la evaluación de la resiliencia de los dispositivos frente a posibles ataques.

Todas las auditorías y pruebas de seguridad de los dispositivos médicos en entornos productivos serán gestionadas exclusivamente por la entidad contratante, ya sea directamente o mediante la contratación de auditores externos.

Asimismo, la entidad contratante se reserva el derecho de llevar a cabo auditorías de cumplimiento sobre los servicios prestados por el adjudicatario para garantizar que dichas tecnologías se ajustan a los requisitos legales, técnicos y normativos aplicables en el entorno sanitario

10.20.3. Pruebas de Validación Post-Despliegue

El adjudicatario deberá realizar, en caso de ser requerido y siempre bajo la supervisión y validación de la entidad contratante, pruebas de validación posteriores al despliegue para todos los dispositivos IoMT y sistemas asociados que sean instalados, configurados o actualizados en el marco del presente

Es copia auténtica de documento electrónico

contrato.

Estas pruebas tendrán como objetivo verificar la correcta operatividad funcional, garantizar la integración segura con la infraestructura sanitaria, evaluar la estabilidad del sistema y confirmar la ausencia de vulnerabilidades o fallos de configuración que puedan generar interferencias o impactos no deseados en los servicios clínicos.

10.21. Formación y concienciación en ciberseguridad

10.21.1. Programas de Formación

El adjudicatario contará con programas de formación en ciberseguridad para todos sus empleados implicados con alguno de los siguientes aspectos: diseño, soporte o mantenimiento de dispositivos, sistemas y servicios relacionados con IoMT.

La formación debe cubrir los fundamentos de la ciberseguridad, la protección de datos, el reconocimiento de amenazas comunes y las políticas de seguridad de la organización.

Los programas ofrecerán una formación continua y actualizaciones periódicas sobre nuevas amenazas y mejores prácticas de seguridad.

10.21.2. Concienciación de Seguridad

De igual forma, el adjudicatario mantendrá campañas de concienciación regulares para todos los empleados, incluyendo aquellos implicados en el diseño, soporte o mantenimiento de soluciones IoMT, con la finalidad de reducir el riesgo humano como vector de ataque en entornos clínicos y tecnológicos sensibles.

Dicha concienciación deberá incluir contenidos prácticos sobre identificación y prevención de ataques de phishing, suplantación de identidad, ingeniería social, manipulación de correos electrónicos, uso indebido de dispositivos móviles o USB, navegación segura, y riesgos derivados de accesos remotos inseguros o credenciales compartidas.

Análogamente, se fomentará además el reporte inmediato de incidentes sospechosos, errores operativos o accesos no autorizados.

10.22. Protección física de los dispositivos

10.22.1. Protección Física de los Dispositivos

Cuando el adjudicatario actúe como fabricante del dispositivo, deberá establecer las medidas de protección física de los dispositivos IoMT, de acuerdo con la criticidad del procesamiento de datos y el entorno de operación.

Estas medidas podrán incluir, entre otras: ubicación en espacios controlados o restringidos, anclaje físico o fijación segura, uso de armarios o cerramientos con llave, identificación clara del equipo, señalización de advertencia y supervisión del cumplimiento de las condiciones técnicas recomendadas por el fabricante (temperatura, humedad, interferencias electromagnéticas, etc.).

El conjunto de medidas de protección deberá cumplir con la regulación aplicable en materia de protección de instalaciones e infraestructuras.

Asimismo, en el caso de implementar dispositivos IoMT, el adjudicatario deberá informar a la entidad contratante sobre las directrices del fabricante, garantizando que los dispositivos IoMT objeto del contrato estén protegidos contra manipulaciones no autorizadas.

Es copia auténtica de documento electrónico

Paralelamente, el adjudicatario deberá colaborar con el personal técnico y de seguridad de la entidad contratante, si es requerido, en la implementación de políticas y procedimientos físicos de control de accesos a salas técnicas, armarios de red, zonas clínicas u otras ubicaciones donde se encuentren operativos los dispositivos, sistemas y servicios relacionados con IoMT.

10.23. Comunicaciones seguras

10.23.1. Configuración de Redes y Comunicaciones

El adjudicatario deberá informar a la entidad contratante sobre los requisitos de seguridad establecidos por el fabricante para la configuración de firewalls, tanto a nivel perimetral como local, y para la correcta protección del entorno operativo de los dispositivos IoMT.

Esta información permitirá que los responsables de la entidad puedan controlar, limitar y monitorizar el tráfico de red intercambiado entre los dispositivos, sistemas y servicios relacionados con IoMT en el marco del presente contrato con otros sistemas, plataformas o servicios externos, garantizando la confidencialidad, integridad y disponibilidad de la información transmitida.

Además, deberá proporcionar los requisitos y recomendaciones de seguridad del fabricante, incluyendo aspectos como segmentación de red, listas blancas, bastionado, protocolos de comunicación, puertos permitidos y cualquier otra medida necesaria para la seguridad del entorno operativo.

No obstante, la implementación de estas medidas en el entorno operativo corresponde a la entidad contratante.

Por otro lado, el adjudicatario deberá notificar cualquier actualización de los requisitos de seguridad que pueda afectar a la configuración de firewalls y del entorno operativo, asegurando que la entidad contratante pueda mantener la protección de los dispositivos y sistemas conforme a las últimas recomendaciones del fabricante y en cumplimiento con la regulación aplicable.

10.24. Protección de la información

10.24.1. Medidas de Seguridad para la Protección de Datos

El adjudicatario deberá aplicar las medidas técnicas y organizativas apropiadas para impedir accesos no autorizados, evitar filtraciones o usos indebidos de datos personales, garantizar la trazabilidad de las operaciones sobre información sensible, y colaborar con la entidad contratante en el cumplimiento de los derechos de los interesados, la gestión de brechas de seguridad y la realización de evaluaciones de impacto en protección de datos cuando así se requiera.

Los dispositivos, sistemas y servicios relacionados con IoMT deberán estar en disposición de asegurar el cumplimiento con las regulaciones de protección de datos como el RGPD y la Ley 3/2018 LOPDGDD que protegen la privacidad de los datos del paciente y la confidencialidad de los datos sensibles.

En particular, debido a la sensibilidad de la información clínica tratada por los dispositivos, deberán disponer obligatoriamente de capacidades de cifrado de datos en tránsito y en reposo, utilizando mecanismos robustos y autorizados por el Centro Criptológico Nacional (CCN), asegurando así la integridad y confidencialidad de la información tratada.

Es copia auténtica de documento electrónico

10.25. Interoperabilidad segura con microservicios

10.25.1. Configuración segura de APIs

En los casos en que los dispositivos IoMT suministrados o el desarrollo del servicio por parte del adjudicatario requieran el uso o creación de APIs para la comunicación con otros microservicios, se deberán implementar las siguientes medidas de seguridad:

Se deberán emplear mecanismos seguros de autenticación, como JSON Web Tokens (JWT) o API Keys.

Cada suscripción o integración con la API deberá contar con un Client_id y Client_secret únicos. Estos valores deberán mantenerse confidenciales y nunca deben incluirse en código fuente accesible públicamente ni en aplicaciones desplegadas.

Toda interacción con la API deberá realizarse a través del protocolo HTTPS, utilizando TLS en su versión 1.3 o superior.

Implementar controles de tasa para limitar el número de solicitudes y mitigar posibles ataques de fuerza bruta o abuso de servicio.

Los mensajes de error deberán evitar la exposición de información sensible del sistema, limitándose a comunicar lo estrictamente necesario.

10.26. Protección de los soportes de información

10.26.1. Devolución y Destrucción de Datos

El adjudicatario, en el caso de llevar a cabo tratamiento de datos personales durante la prestación de los servicios, deberá disponer de mecanismos que regulen la devolución de la información en el formato de datos y los plazos especificados, o en su defecto, la destrucción de los mismos, proporcionando evidencias certificadas de la realización.

Además, deberá seguir el protocolo definido por la entidad contratante para la devolución y destrucción de datos que incluya.

Asimismo, el adjudicatario o terceros en el caso de proceder a destruir un soporte o cualquier otro elemento relacionado con un sistema de información deberá de disponer de un certificado de destrucción o borrado seguro emitido por una entidad acreditada garantiza la trazabilidad y conformidad legal del proceso, asegurando que la información sensible ha sido eliminada de forma irreversible y conforme a los estándares de protección de datos.

10.27. Integración segura con aplicaciones móviles

10.27.1. Permisos y funcionalidades limitadas

El adjudicatario deberá garantizar que todas las aplicaciones móviles que estén sincronizadas, vinculadas o integradas con dispositivos IoMT se desarrollen, configuren y puedan operarse con una política de permisos mínimos y funcionalidades estrictamente limitadas al uso clínico o técnico necesario, conforme a los principios de seguridad desde el diseño y por defecto.

Las aplicaciones móviles no deberán solicitar, acceder ni procesar más información o funciones del dispositivo móvil de lo estrictamente imprescindible.

Queda expresamente prohibido el uso de permisos excesivos o no justificados, tales como el acceso continuo al micrófono, cámara, ubicación, sensores del dispositivo móvil, o la recopilación de

Es copia auténtica de documento electrónico

información biométrica, salvo que esté debidamente justificado, documentado, autorizado por la entidad contratante y alineado con el consentimiento del usuario en los casos en que sea requerido.

También, el adjudicatario deberá asegurar que estas aplicaciones sanitarias incorporen mecanismos seguros de autenticación, cifrado de comunicaciones, control de sesiones activas, y registro de acciones (logs), así como medidas para evitar la manipulación, ejecución de código no autorizado o el acceso no controlado a la información clínica o funcional.

Cualquier funcionalidad de sincronización con el dispositivo IoMT deberá estar limitada, trazada y validada, y no podrá alterar parámetros críticos de funcionamiento del dispositivo salvo que esté autorizado expresamente por la entidad contratante.

La entidad contratante se reserva el derecho de auditar las funcionalidades de las aplicaciones móviles y sus permisos en cualquier momento, así como de exigir su modificación o desactivación si se detectan desviaciones respecto a los principios aquí establecidos.

10.27.2. Restricción de distribución de la aplicación en markets no autorizados

El adjudicatario se compromete a garantizar que las aplicaciones móviles asociadas a los dispositivos IoMT únicamente estén disponibles en tiendas oficiales y autorizadas por la entidad contratante, salvo que se acuerde expresamente otro canal controlado como, por ejemplo, distribución empresarial o MDM.

Queda estrictamente prohibida la publicación, distribución o disponibilidad de dichas aplicaciones en markets no autorizados, alternativos o de terceros que no garanticen el cumplimiento de estándares de seguridad, privacidad y control de versiones.

10.28. Transferencia de la información

10.28.1. Transferencia de Conocimiento e Información al Finalizar el Contrato

Al término del contrato, ya sea por cumplimiento del plazo de vigencia, rescisión anticipada o cualquier otra causa, el adjudicatario estará obligado a llevar a cabo una transferencia ordenada, completa y documentada del conocimiento, la información técnica y los activos digitales relacionados con los dispositivos, plataformas o servicios IoMT que hayan sido suministrados, mantenidos o gestionados durante la vigencia contractual.

Esta transferencia incluirá, como mínimo, toda la documentación técnica actualizada (manuales, configuraciones, claves de administración si procede, topologías, inventario de dispositivos, informes de mantenimiento y seguridad), registros de eventos e incidentes, credenciales bajo control seguro, logs, licencias, esquemas de integración, así como cualquier conocimiento tácito o explícito necesario para garantizar la continuidad operativa, la seguridad funcional y la posibilidad de asumir la gestión por parte de la entidad contratante o de un nuevo proveedor.

La entrega deberá realizarse en formatos estructurados, legibles, verificables y sin restricciones tecnológicas o contractuales que impidan su reutilización.

Asimismo, el adjudicatario se compromete a garantizar que toda la información generada o gestionada en el marco del contrato, incluyendo aquella compartida con terceros subcontratados o proveedores externos, esté debidamente clasificada, protegida y tratada conforme a su nivel de sensibilidad.

Cualquier acuerdo suscrito entre el adjudicatario y terceros que implique el acceso, tratamiento o

Es copia auténtica de documento electrónico

custodia de dicha información deberá incluir cláusulas explícitas que aseguren la clasificación, confidencialidad, integridad y trazabilidad de la misma, alineadas con las políticas de seguridad de la entidad contratante, el ENS, el RGPD, y estándares como ISO/IEC 27001 o ISO 27701.

10.29. Resolución de conflictos en la aplicación de las cláusulas de seguridad

10.29.1. Equilibrio Funcionalidad y Seguridad

Siempre que el adjudicatario considere que la aplicación de alguna de las cláusulas de seguridad establecidas pueda afectar de manera significativa a la disponibilidad de los servicios prestados por los dispositivos IoMT, comprometer su rendimiento o poner en riesgo la seguridad del paciente, deberá notificarlo de forma inmediata y por escrito a la entidad contratante.

Dicha notificación deberá incluir una descripción detallada del motivo de la excepción, los impactos esperados, y la cláusula o cláusulas implicadas.

La entidad contratante evaluará la solicitud presentada por el adjudicatario, considerando las razones expuestas y la documentación aportada, con el fin de determinar si la excepción solicitada está debidamente justificada.

Esta evaluación se realizará conforme a los criterios técnicos y de seguridad aplicables, asegurando que no se comprometa la calidad, disponibilidad o seguridad de los servicios objeto del contrato.

No obstante, la aceptación de una excepción quedará condicionada a que el adjudicatario proponga medidas compensatorias alternativas, las cuales deberán ser documentadas y justificadas, así como garantizar un nivel de seguridad equivalente o superior al establecido por la cláusula objeto de la excepción.

Además, la entidad contratante aprobará dichas medidas compensatorias siempre que estas no supongan un incremento del riesgo del paciente o del entorno asistencial, y que resulten técnicamente viables y verificables.

Toda excepción aceptada, así como las medidas compensatorias aprobadas, deberán quedar documentadas formalmente y registrarse en repositorio centralizado de la entidad contratante, garantizando su trazabilidad durante toda la vigencia del contrato.

Es copia auténtica de documento electrónico