



*Este documento se ha obtenido directamente del original, que contenía todas las firmas auténticas, y se han ocultado los datos personales y los códigos que permitían acceder al original.*

# CONTROL Y SEGURIDAD DE EQUIPOS CONECTADOS A LA RED DE COMUNICACIONES DEL SERMAS

Prescripciones Técnicas

## Contenido

<b>CLÁUSULA 1º - OBJETO.....</b>	<b>3</b>
<b>CLÁUSULA 2º - ALCANCE .....</b>	<b>3</b>
<b>CLÁUSULA 3º - REQUISITOS TÉCNICOS .....</b>	<b>4</b>
<b>3.1 Requisitos generales.....</b>	<b>4</b>
<b>3.2 Requisitos de arquitectura .....</b>	<b>7</b>
<b>3.3 Requisitos de seguridad .....</b>	<b>9</b>
<b>3.4 Datos relativos a tráfico mínimo a considerar en cada ubicación .....</b>	<b>10</b>
<b>3.5 Garantía avanzada del fabricante .....</b>	<b>12</b>
<b>CLÁUSULA 4º - DESCRIPCIÓN DE LOS SERVICIOS .....</b>	<b>13</b>
<b>4.1 Servicios de implantación .....</b>	<b>13</b>
<b>4.2 Servicios de administración y aseguramiento de la monitorización y la calidad de la solución.....</b>	<b>14</b>
<b>CLÁUSULA 5º - -PLAZOS.....</b>	<b>17</b>
<b>CLÁUSULA 6º - RECURSOS APORTADOS POR EL ADJUDICATARIO .....</b>	<b>19</b>
<b>CLÁUSULA 7º - ACUERDOS DE NIVEL DE SERVICIO .....</b>	<b>20</b>

## CLÁUSULA 1º - OBJETO

El objeto del presente documento es establecer los requisitos técnicos mínimos que han de regir los servicios de **suministro, configuración e instalación avanzada de un sistema de control y seguridad de equipos conectados** a la red de comunicaciones de los centros de Atención Primaria del SERMAS. Con ello se quiere facilitar el cumplimiento de los objetivos marcados en línea 6 de la inversión 3 del componente 11 del Plan de Recuperación, Transformación y Resiliencia orientada al Plan de Transformación Digital de la Atención Primaria y comunitaria.

En particular, el objetivo perseguido es ofrecer una atención sanitaria de calidad, **en condiciones de ciberseguridad**.

## CLÁUSULA 2º - ALCANCE

El presente documento de licitación sirve a la contratación de soluciones de control y seguridad de equipos conectados a la red de comunicaciones de los centros de atención sanitaria del SERMAS.

En los últimos años se ha producido un importante aumento de los ciberataques dirigidos contra el sector sanitario español, con graves consecuencias como el cese total o parcial de su actividad. Las áreas susceptibles de ataques de los centros sanitarios se amplían constantemente por el incremento del número de interfaces de comunicación y dispositivos médicos conectados que se utilizan, a esta mayor superficie de ataque, se añade una deficiente segmentación de la red, controles de acceso débiles y dependencia de sistemas obsoletos.

En este sentido, surge la necesidad de garantizar la ciberseguridad en un entorno con un gran número de dispositivos médicos de naturaleza heterogénea conectados a la red corporativa y manejando información médica de los pacientes.

Por otro lado, los Centros de Operaciones de Seguridad (SOC) están ya consolidados en Tecnología de la Información (TI). Sin embargo, la realidad de los centros sanitarios o de los sistemas industriales es distinta. Igualmente, cada vez hay más dispositivos conectados a la red y, por tanto, sometidos a amenazas de ciberseguridad, pero los ataques a este tipo de dispositivos son susceptibles de causar pérdidas de vidas humanas o daños en las mismas. Esto hace que, en estos entornos es preciso asegurar la continuidad del servicio a prestar, además de preocuparse por la confidencialidad, integridad, disponibilidad o autenticidad de la información.

Un SOC que deba gestionar este tipo de dispositivos (IoMT, OT o IoT en general) sigue debiendo gestionar las alertas de seguridad, respondiendo a incidentes, conocer y gestionar las vulnerabilidades o recuperar la operativa. Sin embargo, las herramientas difieren. El SOC no tiene, en muchas ocasiones, documentación sobre dispositivos, sistemas o procesos, y para asegurar la continuidad del servicio no puede ser intrusivo y necesita mejores herramientas para clasificar los activos. El objetivo final es poder identificar los riesgos derivados de esos equipos conectados y establecer las medidas de seguridad necesarias que eviten una exposición innecesaria, como consecuencia de esos riesgos, especialmente por no contar con software o configuraciones actualizadas.

El ámbito de actuación de este contrato abarcará la implantación y soporte de un sistema de control y seguridad de equipos conectados, enfocado en el ámbito sanitario. Este sistema estará encargado de la captación de los datos relevantes de comportamiento de los dispositivos ubicados en las redes sanitarias, el inventario y la clasificación automática de los mismos por tipologías, de sus datos relevantes (ubicación, sistema operativo, firmware, versión), sus vulnerabilidades a nivel de ciberseguridad, su posible grado de infección y, en general, la detección y priorización de los riesgos de ciberseguridad, así como la posibilidad de tomar contramedidas de carácter preventivo o reactivo locales a los centros. Para ello, será preciso un suministro y configuración inicial, unos servicios avanzados de configuración e integraciones y el

diseño y prueba del sistema de monitorización y aseguramiento de la calidad. En resumen, el sistema a implantar debe conseguir los siguientes objetivos:

- Visibilidad, inventario, detección y clasificación de activos de forma continua. Es preciso monitorizar los equipos conectados en tiempo real.
- Gestión preventiva de riesgos:
  - o Detección de vulnerabilidades. Es preciso conocer el nivel de seguridad y vulnerabilidades que afectan a los dispositivos, para mejorar la seguridad de forma continua.
  - o Detección de amenazas y ataques
- Capacidad de respuesta a ataques, que puede realizarse de dos formas, no necesariamente alternativas:
  - o enriqueciendo los datos de los SIEM, para mejorar la observabilidad de la red
  - o mediante integraciones con un NAC y/o con los cortafuegos de cada edificio.

En el alcance del contrato estarán incluidas, globalmente las **licencias/subscripciones**, el **soporte** y **garantía** de los fabricantes asociados, para los productos suministrados de captación de información, inventario, clasificación y perfilado, gestión centralizada de la configuración, detección de vulnerabilidades, informes de riesgos, integraciones con los elementos de red y seguridad y analítica. Las licencias o suscripciones suministradas serán **todas** las necesarias para cubrir todos los objetos, dispositivos o usuarios ubicados en los siguientes centros de Atención Primaria y otros que le prestan servicios:

- Los 32 centros hospitalarios indicados en este documento
- Los 2 centros de proceso de datos del SERMAS
- Hasta 30 centros de especialidades
- Hasta 275 centros de salud.

## CLÁUSULA 3º - REQUISITOS TÉCNICOS

### 3.1 Requisitos generales

- REQ 1. Acceso cliente mediante interfaz basada en entorno web multiplataforma, con diseño adaptativo, que permita la visualización en diferentes tipos de dispositivos, y alto nivel de usabilidad compatible con los navegadores Microsoft Edge y Google Chrome.
- REQ 2. Acceso por autenticación con usuario y contraseña, integrado con el directorio activo del organismo.
- REQ 3. El sistema debe permitir el acceso con doble factor de autenticación, al menos basada en SAML, y como mínimo con Microsoft Azure
- REQ 4. Debe ofrecer una integración completa con los directorios activos de la entidad, de forma que se haga más sencilla el alta y baja de usuarios, asignación de roles y habilitar mecanismos de Single Sign On. En este sentido, debe contemplarse desde el inicio que la integración deber realizarse en un escenario de identidades de usuarios y administradores repartidos en dos Directorios Activos Microsoft, entre los que existe una relación de confianza.
- REQ 5. Debe permitir el acceso a todos los módulos de la herramienta a los que tenga acceso (permisos) desde una misma sesión, sin que requiera del usuario múltiples autenticaciones
- REQ 6. Debe permitir el control de roles y perfiles de usuario.
- REQ 7. La herramienta debe contar con un modelo de arquitectura multi-entidad, adecuado a las necesidades de un servicio de salud, incorporando dependencias e interrelaciones entre las diferentes entidades que habitualmente lo componen (servicios centrales, centros de atención primaria, hospitales, etc.).
- REQ 8. La herramienta debe ser capaz de gestionar un sistema multiusuario que facilite realizar perfilado de usuarios en base a módulos/funciones. Este requisito afecta a

paneles de mando, informes y alertas, de forma que puedan particularizarse para los siguientes roles:

- a. Administradores IT (comunicaciones, seguridad perimetral, áreas de informática, ...), con capacidad de ver equipamiento existente, su clasificación, flujos de tráfico, ...
- b. Administradores de Seguridad, con capacidad de conocer el nivel de riesgo del equipamiento, versiones de sistema operativo o sus vulnerabilidades
- c. Profesionales de la Salud, con capacidad de conocer el nivel de uso y productividad de las tipologías asignadas a cada rol

REQ 9. Se requiere un sistema que proporcione una visibilidad de todos los dispositivos, no únicamente **médicos**, sino **IoT, OT e IT**, conectados a la red directa o indirectamente (ethernet cableado, wifi, conversores serie, gateways,...), identificándolos de forma automática, junto con su tipología y características.

REQ 10. La solución no debe requerir la instalación de agentes de ningún tipo en ningún tipo de dispositivo final conectado a la red (IT, OT, IoT, ...)

REQ 11. A la hora de realizar la clasificación, el sistema considerará, al menos, las siguientes categorías de equipos clasificados según naturaleza, para poder cubrir los casos de uso de los entornos en el alcance de este pliego, siendo aceptables clasificaciones que distingan claramente entre IT, OT, IoT y resto de IoT. A partir de ellos se consideran los niveles de categorías, y siendo el siguiente un mínimo de categorías:

- a. Ordenadores, servidores, impresoras
- b. Comunicaciones (telecomunicaciones, equipos de red)
- c. Seguridad
- d. Multimedia, Displays e Imagen genérica
- e. Médicos (IoT)
- f. OT: gestión de edificios, instalaciones y automatismos
- g. IoT genérico
- h. Equipos de mano (*handhelds*): ej: móviles

REQ 12. A la hora de realizar la clasificación, el sistema considerará, al menos, los siguientes equipos, dentro de las anteriores subcategorías:

1. Ordenadores personales
2. Estaciones de trabajo
3. Servidores
4. Hipervisores
5. Máquinas virtuales
6. Servidores de almacenamiento
7. Impresoras
8. Switches/routers
9. Cortafuegos
10. Pasarelas
11. Puntos de acceso Wifi
12. Controladores
13. Equipos de telefonía IP
14. Teléfonos móviles
15. Televisores
16. Angiógrafos
17. Dispensadores médicos
18. ECGs
19. Estaciones de imagen
20. Equipos de laboratorio
21. Estaciones centrales
22. Fluoroscopia
23. Medicina Nuclear
24. Monitores de pacientes

25. PACs
  26. MRIs (Equipos de resonancia magnética)
  27. Rayos X
  28. CR (Radiografía computerizada)
  29. TACs
  30. Radiología en general
  31. Imagen en general
  32. Sistemas de optometría
  33. Ultrasonidos
  34. Mamógrafos
  35. Escáners de productos
  36. Mesas
  37. Gateways de IoT
  38. IoT en general
  39. SBCs
  40. UPS
  41. Switches industriales
  42. Cámaras IP
  43. Luces
  44. Sensores
- REQ 13. La interfaz gráfica deberá estar en idioma **español/castellano**. Excepcionalmente, se puede admitir que los nombres de los grupos y categorías en que se clasifican los dispositivos estén en idioma inglés, dado que suele tratarse de vocablos ampliamente conocidos en esta lengua (computer, display, scanner, IoT, etc)
- REQ 14. Se requiere un sistema que cuente con la capacidad de distinguir entre dispositivos legítimos (conocidos y aprobados) y no inventariados (nuevos).
- REQ 15. El sistema permitirá corregir manualmente, mediante algún procedimiento, los equipos desconocidos, que el propio sistema no haya podido identificar de forma correcta, o mal clasificados.
- REQ 16. El descubrimiento de dispositivos se debe basar en la funcionalidad de DPI, Deep Packet Inspection sin necesidad de integrar directamente dispositivos finales o instalar agentes en los mismos.
- REQ 17. Se requiere que el sistema que cuente con una interfaz gráfica que facilite información completa de la situación de la red de dispositivos.
- REQ 18. El sistema debe permitir el listado los siguientes atributos **mínimos** en la vista de los dispositivos finales conectados en una sede: dirección IP, MAC, IP y/o nombre de switch (o AP) y puerto físico de conexión en switch, VLAN, usuario si procede y tipo de dispositivo clasificado. Para tal fin deberá considerarse la integración de los siguientes fabricantes de switches: HP/Aruba, Extreme/Enterasys y Cisco) y los siguientes fabricantes de infraestructura Wifi: Aruba y Extreme)
- REQ 19. Los **filtrados** para las búsquedas de equipamientos específicos podrán realizarse por centro, naturaleza/categoría/clase/tipo del dispositivo, dirección IP, MAC y VLAN
- REQ 20. Se requiere que el sistema muestre gráficamente el uso de los dispositivos. La solución deberá, por tanto, permitir tener visibilidad del tráfico de los equipos de todo tipo (IoT, OT, IoMT, IT, etc.) conectados a nivel IP en los centros (LAN y Wifi) y de los elementos con que se conectan. Ello permitirá restringir las comunicaciones a nivel de los cortafuegos existentes en los centros.
- REQ 21. La solución deberá contener registros y capacidad de búsqueda por sí misma, para poder conocer todas las comunicaciones desde y hacia los dispositivos conectados en los centros objeto del contrato, identificando tanto el centro como la ubicación física de los dispositivos
- REQ 22. El sistema debe ser capaz de interpretar protocolos de comunicaciones de uso médico. Como mínimo debe poder interpretar HL7 (*Health Level 7*) y DICOM (*Digital Imaging and Communications in Medicine*)



- REQ 23. El sistema debe incorporar capacidades de *reporting* avanzadas que permitan ver la evolución del sistema, faciliten el conocimiento general y de detalle de la situación, así como incorporación de mecanismos de alerta.
- REQ 24. El sistema debe disponer de mecanismos y conservación de trazabilidad, generación de informes, plantillas, control de avisos y notificaciones.
- REQ 25. Debe tener la capacidad de proveer cuadros de mando y herramientas de análisis de datos personalizados. La solución debe contar con la posibilidad de programar cuadros de mando e informes en base a la información tratada y las necesidades del Servicio de Salud.
- REQ 26. La solución debe permitir programar informes mensuales diferenciados por centros e incluso por tipos de usuarios finales de la herramienta.
- REQ 27. La solución deberá contar con la posibilidad de configurar y remitir alertas ante la detección de nuevos riesgos y amenaza en base a los criterios definidos por el cliente.
- REQ 28. Debe tener capacidad de almacenamiento de eventos durante, al menos, 30 días, de tráfico durante 7 días y de logs durante 30 días. Adicionalmente se contará con una funcionalidad de reenvío de logs o eventos a un syslog externo en caso de que el SERMAS considere oportuno un mayor periodo de retención de datos.
- REQ 29. Debe tener capacidad de incorporar mecanismos que ayuden y dinamicen a los profesionales especializados o no en esta cuestión: notificaciones, recordatorios, etc.
- REQ 30. El sistema debe proporcionar información relativa a los tiempos de uso del equipamiento IoMT, con objeto de detectar la infrautilización de los mismos, cuando dichos datos estén disponibles, por ejemplo, por encontrarse dentro de los protocolos DICOM, HL7, etc. Este tiempo de uso no se debe medir por su actividad en la red, sino que se trata de datos de uso real en funciones estrictamente médicas.
- REQ 31. El sistema debe permitir el acceso a la información de uso del equipamiento IoMT a diferentes usuarios en cada uno de los centros, de forma que cada profesional de la salud vea únicamente los equipos que le correspondan.
- REQ 32. La solución será capaz de mostrar gráficamente la utilización de los dispositivos médicos: días, horas, tipo de pruebas, etc. mostrando igualmente el evolutivo de uso. La tendencia deberá abarcar varios días y poder determinar la tendencia respecto a periodos anteriores
- REQ 33. Las características multi-entidad de la solución deben contemplar como mínimo:
- a. La posibilidad de restringir la visibilidad del equipamiento a nivel de entidad, y de tipos de dispositivos a ciertos roles dentro de la entidad
  - b. La posibilidad de corregir, por cada entidad, los activos mal identificados
  - c. La posibilidad de configurar ciertas configuraciones personalizadas
  - d. La posibilidad de configurar informes personalizados
  - e. La posibilidad de que cada entidad cuente con alertas y paneles específicos
  - f. La posibilidad de que la visibilidad, configuraciones o informes puedan ser realizadas por administradores globales

### 3.2 Requisitos de arquitectura

La solución propuesta puede disponer de elementos on-premise y de elementos ofrecidos en Cloud en modo servicio (SaaS).

- REQ 34. Existirá una plataforma de gestión centralizada y redundada, que contemplará al menos los aspectos de visibilidad de equipos, monitorización, informes y alertas. En los aspectos de configuración, se busca, igualmente, evitar en la medida de lo posible, para la operación continua, la configuración equipo a equipo.
- REQ 35. Se solicita una plataforma de gestión con supervivencia ante la caída de un CPD en configuración de HA con supervivencia ante caída de un equipo. Preferiblemente con posibilidad de distribuir entre varios CPDs.

- REQ 36. Debido al previsible incremento de dispositivos IoT en el tiempo, la plataforma de gestión debe ser escalable horizontalmente, sin ser sustituida.
- REQ 37. La solución deberá suministrar **una sonda o colectora local** en cada uno de los 32 centros sanitarios y en cada uno de los **dos CPDs** del SERMAS, debiendo poder ser alojada en bastidores de tamaño 800x800mm.
- REQ 38. Las colectoras locales se suministrarán como un servicio por parte del adjudicatario, de forma que será causa válida para exigir el reemplazo del equipo, el malfuncionamiento por cualquier causa del mismo, incluida la falta de capacidad del equipo para realizar adecuadamente sus funciones durante la duración del periodo por el que se adquiere la garantía extendida del software asociado a las licencias.
- REQ 39. Para el dimensionado de las colectoras locales, los ofertantes tomarán en consideración los datos de la última Memoria Anual de Actividad del Servicio Madrileño de Salud que esté publicada, donde se incluyen indicadores relevantes de actividad o de capacidad. El dato de tráfico esperado en cada centro se suministra más adelante, pero no debe considerarse limitación alguna en el número de objetos, dispositivos o usuarios a controlar. La oferta debe contemplar, dentro de sus servicios de soporte, y sin incremento de coste, la posibilidad de incremento del tráfico en cada ubicación al doble del indicado en la tabla, incluyendo la posible sustitución, ampliación o adición de controladoras locales.
- REQ 40. Las colectoras se conectarán siempre a *Network Packet Brokers* ya existentes en los centros. El adjudicatario suministrará los elementos necesarios para la conexión de estas sondas o elementos auxiliares con los *packet brokers*, lo que incluye tanto el cableado como los posibles transceptores necesarios para realizar estas conexiones en los centros. Igualmente se suministrarán los cables de alimentación de las colectoras o cualquier otro tipo de servidor físico a instalar en cualquier ubicación. Todo el material deberá seguir los estándares de calidad aplicados en el CPD correspondiente.
- REQ 41. Las colectoras deberán realizar un uso muy bajo del ancho de banda para sus comunicaciones con sistemas centrales o ubicados en la nube.
- REQ 42. Para poder cumplir con los requisitos incluidos en este documento:
- En los centros hospitalarios se podrá disponer de la copia del tráfico LAN, mayoritariamente de las conexiones de los cortafuegos, para su procesamiento por la sonda. En algunos casos, para ciertos flujos de tráfico se pueden plantear escenarios de captura de tráfico sFlow para complementar la detección.
  - En los CPDs se podrá disponer de la copia del tráfico procedente de la WAN. A los CPDs del SERMAS se conectan todos aquellos equipos ubicados en los centros de salud y centros de especialidades, y muchos de los equipos ubicados en hospitales, cuyo tráfico ya está siendo capturado por las sondas locales.
- REQ 43. Si la solución requiere de algún servidor central (o servidores) deberá suministrarse en formato hardware, no en formato virtual, y se suministrarán de la misma forma que las sondas locales, en modo servicio, pero asociado al coste de las licencias.
- REQ 44. La solución debe ser capaz de una integración con sistemas, tanto propios del servicio de salud, como externos. En particular:
- Integración con al menos dos directorios activos y/o sistema de gestión de identidades del SERMAS y de la Comunidad de Madrid, respectivamente.
  - Integración con los sistemas de inventario del servicio de salud
  - Integración con las herramientas CCN-CERT,
  - Integración con Aruba Clearpass, NAC utilizado actualmente en el SERMAS, para implementar una segmentación automática de la red e implementar acciones preventivas o reactivas de Seguridad.
  - Integración con los sistemas de switching (SNMP), firewall y SIEM, con objeto de posibilitar alertas, e implementar acciones preventivas o reactivas de Seguridad.
  - Integración con sistemas Monitorización Externos aplicables al entorno de Sanidad.
  - Integración, si se considerara necesario, con el sistema de ticketing BMC Remedy ITSM.



- REQ 45. El sistema deberá ofrecer servicios web y/o APIs para la explotación de información desde otros sistemas de la Comunidad de Madrid.
- REQ 46. La herramienta debe disponer de APIs para facilitar la extracción de los datos de inventario y clasificación y facilitar el enriquecimiento de información por sistemas externos.
- REQ 47. Las colectoras de seguridad locales y las de los CPDs dispondrán de doble fuente de alimentación. En los CPDs podrá requerirse con PDU. En cualquier caso, se suministrará el cableado preciso en cada ubicación sin incremento del coste final.

### 3.3 Requisitos de seguridad

- REQ 48. Se requiere un sistema capaz de proteger los datos y la privacidad del paciente contra ataques malware, ransomware u otros ciberataques avanzados dirigidos a dispositivos médicos conectados a la red.
- REQ 49. Se requiere un sistema que monitorice la red de forma continuada y permita la detección de amenazas y anomalías, extrayendo patrones basados en el comportamiento de las comunicaciones y también detección de amenazas basadas en firmas, que podrían señalar conexiones anómalas o sospechosas.
- REQ 50. La solución deberá ofrecer una visión del estado global de la seguridad del Servicio de Salud y por cada una de las sedes.
- REQ 51. Salvo autorización expresa del contratante, en ningún caso se podrá realizar tratamiento de datos de carácter personal fuera de las instalaciones de la Comunidad de Madrid. En caso de que la solución propuesta por el licitador requiera el tratamiento de datos de carácter personal para su funcionamiento en base a los requerimientos del presente pliego, el adjudicatario deberá incluir en su oferta los tipos de datos que tratará y el tratamiento sobre los mismos. En este caso los transmitirá la información mediante protocolos seguros. En caso de ser necesario realizar conexiones hacia el exterior de la red sanitaria o institucional de la Comunidad de Madrid, dichas comunicaciones serán cifradas y asegurarán un nivel de seguridad alta según el ENS.
- REQ 52. El sistema no almacenará datos personales de salud (PHI) en ningún caso.
- REQ 53. Se requiere un sistema que identifique riesgos y vulnerabilidades basadas en IoTs, CVEs, etc, de los dispositivos detectados sin necesidad de lanzar análisis de vulnerabilidades que puedan impactar sobre el equipamiento. El sistema incluirá la realización de recomendaciones de red para reducir el riesgo.
- REQ 54. De forma deseable, la solución debe detectar, basándose en el tráfico analizado, anomalías de comportamiento, ya sean basados en la función del dispositivo como en el comportamiento de equipamientos conectados en el mismo centro, con la misma tipología.
- REQ 55. Al detectar una vulnerabilidad, la alerta de seguridad debe identificar al equipo, y, si está disponible, su sistema operativo y versión, identificar la vulnerabilidad y describirla, asignarle una relevancia o criticidad y una probabilidad de explotación.
- REQ 56. Se requiere un sistema que categorice las amenazas y vulnerabilidades, estableciendo un nivel de riesgo del dispositivo basado en la probabilidad y severidad del impacto desde el punto de vista de la confidencialidad, integridad y disponibilidad. Asimismo, dispondrá de una clasificación del dispositivo de acuerdo a la criticidad del servicio sanitario. La combinación de ambos criterios resultará en la recomendación de unas medidas de actuación, proporcionando una visión centralizada del grado de exposición y riesgo.
- REQ 57. Para clasificar la criticidad de las vulnerabilidades el sistema seguirá el sistema CVSS (*Common Vulnerability System Score*) dependiente del FIRST (*Forum of Incident Response and Security Teams*)
- REQ 58. La probabilidad de explotación de una vulnerabilidad en los próximos 30 días será evaluada por el sistema utilizando EPSS v3 (*Exploit Prediction Score System*), gestionada

también por el FIRST, con el objetivo de maximizar la cobertura y eficiencia en la identificación y priorización de la remediación de vulnerabilidades.

- REQ 59. La solución deberá cumplir con los requisitos de almacenamiento y salvaguarda de información para garantizar el cumplimiento regulatorio español, principalmente ENS y RGPD/LOPD y GDD. En este sentido, si la solución estuviera basada en nube, el colector enviará los datos y metadatos necesarios a la nube del fabricante para realizar el análisis de esos datos. En este caso, el envío se realizará garantizando el cumplimiento del RGPD
- REQ 60. El sistema facilitará información del nivel de cumplimiento de seguridad respecto a determinadas normas o estándares internacionales o nacionales o políticas de cumplimiento de organizaciones internacionalmente. Se valorará que entre esas normas se encuentre el Esquema Nacional de Seguridad.
- REQ 61. El sistema permitirá descargar la información MDS2 de cada dispositivo, siempre que dicho dispositivo cuente con ella.
- REQ 62. La solución, al menos en el caso de los dispositivos IoMT, debe proporcionar información relativa al tipo de tratamiento de datos personales de salud, permitiendo diferenciar los dispositivos que tratan con información sensible de aquellos que no lo hacen para tomar posibles decisiones en base a esa información.
- REQ 63. Se requiere un sistema que esté permanentemente actualizado en cuanto a la incorporación de nuevos dispositivos detectables.
- REQ 64. Se requiere un sistema que esté permanentemente actualizado en cuanto a la detección de nuevas vulnerabilidades y corrección en sus propios sistemas de información de las mismas.
- REQ 65. En caso de requerirse componentes en nube pública, éstos deberán ser proporcionados, gestionados, actualizados y securizados por el fabricante. En cualquier caso, dicha nube debe encontrarse en un centro de proceso de datos ubicado en la Unión Europea, cuyo proveedor cuente con la certificación de nivel **alto** del Esquema Nacional de Seguridad.
- REQ 66. La información de seguridad generada por el sistema podrá utilizarse para generar Respuestas Automatizadas por la propia solución en tres modalidades:
- h. Recomendación de actuaciones concretas a realizar sobre la red o mecanismos de seguridad de esta (NAC y FW)
  - i. Actualización dinámica de direcciones IP de efecto casi-inmediato sobre reglas de seguridad previamente definidas en cortafuegos
  - j. Actualización dinámica en grupos de objetos de sistemas NAC.
- REQ 67. Debe poder consumir inteligencia de amenazas desde dentro y fuera de la organización. Esta inteligencia debe ayudar a detectar posibles amenazas en el tráfico de la red y se debe poder compartir con otras soluciones de seguridad.
- REQ 68. La plataforma debe utilizar múltiples fuentes de IoCs para ayudar a identificar ataques y anomalías en tiempo real y, en su caso, generar una alerta que incluya los IoCs que activaron la alerta, para que puedan ser consumidos por otras herramientas, como pueden ser sistemas SIEM
- REQ 69. permitir la gestión y compartición de IOCs (sha1, sha256, URLs, dominios, Dirección IP, correos electrónicos).
- REQ 70. La solución debe crear una fuente de alertas de seguridad que indiquen el tráfico de red sospechoso y potencialmente malicioso.

### 3.4 Datos relativos a tráfico mínimo a considerar en cada ubicación

A continuación, se indican las necesidades de procesamiento de tráfico de las colectoras en cada ubicación, y la velocidad de interfaz de red requerida en caso de suministrarse un único equipo por ubicación.



	tráfico colector/ interfaz de red (Gb/s)
Hospital Universitario La Paz	6/10
Hospital Universitario La Paz - Cantoblanco	2/10
Hospital Universitario La Paz - Carlos III	2/10
Hospital de Emergencia Enfermera Isabel Zendal	2/10
Hospital Universitario 12 de Octubre	6/10
Hospital Universitario Ramón y Cajal	6/10
Hospital General Universitario Gregorio Marañón	6/10
Hospital Universitario de La Princesa	4/10
Hospital Infantil Universitario Niño Jesús	2/10
Hospital Clínico San Carlos	6/10
Hospital Universitario Príncipe de Asturias	4/10
Hospital Universitario de Getafe	3/10
Hospital Universitario de Móstoles	3/10
Hospital Central de la Cruz Roja San José y Santa Adela	2/10
Hospital Universitario Santa Cristina	2/10
Hospital El Escorial	0,9/1
Hospital Doctor Rodríguez Lafora	0,9/1
Hospital La Fuenfría	2/10
Hospital Universitario Severo Ochoa	3/10
Hospital Virgen de la Poveda	0,9/1
Hospital de Guadarrama	0,9/1
Hospital Universitario Fundación Alcorcón	3/10
Hospital Universitario José Germain	0,9/1
Hospital Universitario de Fuenlabrada	3/10
Hospital Universitario Puerta de Hierro Majadahonda	4/10
Hospital Universitario del Henares	2/10
Hospital Universitario del Sureste	2/10
Hospital Universitario del Tajo	2/10
Hospital Universitario Infanta Cristina	2/10
Hospital Universitario Infanta Leonor	2/10
Hospital Virgen de la Torre	0,9/1
Hospital Universitario Infanta Sofía	2/10
CPD1	9/40
CPD2	9/40

Para cumplir con los requisitos se deben ofrecer las siguientes licencias:

Descripción Licencia	Unidades
Licencias y garantía extendida para centros sanitarios (hospitalario), incluyendo las 32 colectoras	32
Licencias y garantía extendida para centros de salud y especialidades (no hospitalario), incluyendo las 2 colectoras de los CPDs e integraciones	305
<b>SUBTOTAL SUMINISTROS</b>	<b>337</b>

Las colectoras en CPD darán cobertura al tráfico originado por los dispositivos ubicados en centros de salud y centros de especialidades.

No se podrán instalar elementos hardware de los cuales el fabricante haya anunciado una fecha de fin de venta. En el caso de que saliera de soporte un equipo o componente software durante la vigencia de las licencias, deberá ser sustituido por el adjudicatario sin coste.

Las colectoras incluirán los transceptores necesarios para atender en cada ubicación los tráficos mínimos indicados en este apartado. Igualmente incluirá el cable en cobre o fibra desde la colectoras al Network Packet Broker que le replicará el tráfico.

### 3.5 Garantía avanzada del fabricante

En el alcance del contrato estarán incluidas, globalmente las **licencias**, que incluyen la **garantía extendida** del adjudicatario por un periodo mínimo de **4 años**, para los productos suministrados de captación de información, inventario, clasificación y perfilado, gestión centralizada de la configuración, detección de vulnerabilidades, informes de riesgos, integraciones con los elementos de red y seguridad y analítica. Las licencias suministradas serán **todas** las necesarias para cubrir todos los objetos, dispositivos o usuarios ubicados en los siguientes centros de Atención Primaria y otros que le prestan servicios:

- Los 32 centros hospitalarios indicados en este documento
- Los 2 centros de proceso de datos del SERMAS
- Hasta 30 centros de especialidades
- Hasta 275 centros de salud.

Debido a la existencia de entregas parciales y la necesidad de coordinación del siguiente contrato como un todo, los centros incluidos en la última entrega tendrán una licencia con vigencia mínima de 4 años, y la vigencia de las licencias de los centros incluidos en las entregas previas finalizarán con la expiración de la vigencia de las licencias de los centros del último hito. A tal efecto, el certificado de conformidad del último hito incluirá la fecha de suministro de las licencias (configuración básica) de forma diferenciada de los servicios avanzados. La vigencia del 100% de las licencias expirará exactamente 48 meses naturales después, o después en caso de mejora.

Los programas deben suministrarse bajo alguna modalidad de licenciamiento tal, que garantice al menos los siguientes **derechos ante el fabricante**:



Programa	Derechos durante la vigencia de las licencias
Programas bajo la modalidad de licenciamiento incluida en esta licitación	<ul style="list-style-type: none"> <li>• Derecho de uso: por todos los dispositivos de cada centro</li> <li>• Derecho de actualización: parches de seguridad, versiones menores, versiones mayores, otros...</li> <li>• Derecho de acceso a documentación: manuales, guías para operación, soporte y/o integración</li> <li>• Derecho de consulta al fabricante (soporte del fabricante): <ul style="list-style-type: none"> <li>○ Horario: 8x5 (mínimo)</li> <li>○ Tiempo de respuesta: 5 días laborables, o más estricto</li> <li>○ Otros aspectos: Comunicación en español/castellano</li> </ul> </li> <li>• Otros derechos:</li> </ul>

## CLÁUSULA 4º - DESCRIPCIÓN DE LOS SERVICIOS

### 4.1 Servicios de implantación

El periodo de implantación comenzará tan pronto como el adjudicatario informe de que puede entregar el material para el primer centro y finalizará con la obtención del certificado de conformidad para el último centro. Normalmente requerirá la estrecha colaboración del fabricante.

El adjudicatario será responsable del suministro, etiquetado, instalación en sede y configuración de equipos y servicios existentes, siguiendo las premisas técnicas que determine Madrid Digital y la D.G. de Salud Digital.

Para cada centro, una vez estén instaladas las colectoras locales e integradas en el sistema global, durante esta fase se producirá la clasificación automática y manual de todos los equipos conectados y la elaboración de los informes de seguridad iniciales de cada centro, así mismo, se deberá diseñar los procedimientos de actualización y soporte, que deberán probarse durante la ejecución del contrato hasta que esté realizada la última de las instalaciones avanzadas del proyecto, garantizando así que tanto los procesos como el sistema de soporte definidos son correctos y compatibles con el conjunto del sistema.

Estas tareas están destinadas a garantizar una puesta en marcha efectiva de la instalación, comprobar la corrección de las integraciones, así como, generar la documentación y los procesos necesarios y realizar las pruebas pertinentes de todo el conjunto.

La clasificación automática dependerá de las capacidades de la herramienta, para las cuales se estipula un ANS, y la clasificación manual:

- Puede precisar de servicios del fabricante para efectuar la reclasificación, los dispositivos de electromedicina constituyen una tipología diferenciada.
- El área de informática de cada hospital podrá reportar antes del fin de la instalación avanzada la clasificación errónea de algunos dispositivos, que deberán ser corregidos,
- en última instancia, podría ser precisa la ayuda del área de informática de cada hospital para alcanzar el ANS mínimo para dar por finalizado un centro.

En general, estos servicios de clasificación conllevan unos Acuerdos de Nivel de Servicio incluidos en el apartado 8 de este documento.

Antes de los trabajos de finalización de la implantación en cada centro se entregará la documentación asociada a la configuración básica y se reflejará en acta:

- El grado de cumplimiento de los ANS para ese centro concreto.
- Un informe resumen de la primera auditoría de dispositivos detectados, incluyendo la cantidad de cada tipo de dispositivos. El formato de informes y tipos de dispositivos a incluir se decidirá con anterioridad.
- Un informe de vulnerabilidades y riesgos detectados, así como una priorización de los riesgos a mitigar

Para llevar a cabo los servicios necesarios, los técnicos encargados de estos servicios deberán tener un soporte adecuado (back office) por parte del fabricante para las incidencias que puedan surgir hasta la aceptación de la instalación por la D.G. de Salud Digital.

## **SUMINISTRO Y CONFIGURACIÓN BÁSICA**

El adjudicatario será responsable de la revisión previa de la infraestructura física y facilidades del inmueble para la instalación.

Al existir equipos que se ubican en cada centro en modo servicio, la puesta en marcha inicial, dentro de la configuración básica, se requiere la realización de las siguientes tareas:

- Gestión del proyecto
- Toma de datos sobre requerimientos
- Planificación
- Replanteo
- Etiquetado e instalación física de los equipos
- Cableado
- Actualización de versiones y configuración inicial, incluyendo la posible actualización y aplicación de plantillas

## **DOCUMENTACIÓN DE LA CONFIGURACIÓN BÁSICA**

- Documentación de la instalación en cada centro:
  - información detallada de equipos físicos conectados,
  - sus modelos, números de serie, etiqueta de inventario,
  - conexión físico y lógico,
  - versión de sistema operativo o firmware
- Con la primera entrega, deberá incluirse la Guía de operación, incluyendo:
  - las tareas asociadas al descubrimiento automático de dispositivos y su recategorización manual
  - las tareas asociadas a integrar la herramienta con nuevos switches, controladoras wifi o cortafuegos
  - las tareas relacionadas con búsquedas de dispositivos y localización física de los mismos
  - las tareas de generación automatizada de informes
  - las tareas asociadas a la actualización de versiones, aunque sean responsabilidad del adjudicatario
  - las tareas asociadas a la inclusión de un nuevo centro o una nueva red

Dicha guía de operación se irá actualizando durante el periodo de duración del servicio de Instalación Avanzada, en función de las carencias que se vayan detectando.

## **4.2 Servicios de administración y aseguramiento de la monitorización y la calidad de la solución**

### **DISEÑO Y PRUEBA DE LOS SISTEMAS DE MONITORIZACIÓN**

Como parte de los servicios de instalación avanzada, se deben considerar los siguientes tipos de actividades para las cuales se deberá diseñar los procesos asociados y definir un conjunto de pruebas para la verificación de su validez durante el tiempo que se realiza todo el conjunto de instalaciones del sistema:

- Respuesta a peticiones y consultas, que sean solicitados por los interlocutores identificados en los campos de Comunicaciones, Seguridad y Servicio Madrileño de Salud. Por ejemplo, la provisión de roles y accesos, la generación de aquellos informes y auditorías, la reclasificación de dispositivos, o los cambios de configuración necesarios para mantener las integraciones necesarias para el correcto funcionamiento de la solución.



- Monitorización, supervisión de alertas generadas por el propio sistema y los dispositivos conectados, y atención a incidencias durante un horario de 8x5 en días laborables, o superior. Deberá quedar definido un procedimiento de actuación, diferenciando según su tipología, ante:
  - la conexión de nuevos equipos, diferenciando según su tipología,
  - la detección de tráfico indeseado
  - la detección del uso de contraseñas débiles
  - la detección de vulnerabilidades de los equipos conectados
- Resolución de incidencias del propio sistema, de sus equipos, o de las integraciones y, en general, la resolución de problemas de todo tipo.
- El aseguramiento para mantener siempre actualizados el inventario de dispositivos conectados, su categorización y detectada su conexión a switch o punto de acceso wifi.
- En los casos que se defina, realización del escalado proactivo de eventos de seguridad al SOC, ya sea de forma automática desde la herramienta o manual a través de los sistemas de comunicación que se definan.
- Extracción y distribución de informes mensuales de:
  - Grado de cumplimiento de los ANS.
  - Número total de dispositivos con una clasificación a alto nivel: IT, IoMT, IoT...
  - Informe de riesgos por tipo de dispositivo, fabricante, grupo de vulnerabilidad y localización, con priorización de los activos/servicios con riesgos a mitigar en función de la gravedad, su probabilidad de explotación y el contexto clínico.
  - Identificación de incidentes de seguridad. Con los siguientes datos: descripción del incidente, severidad, conexiones, flujo de datos, eventos...
  - Análisis del porcentaje de utilización de los dispositivos médicos y presentación de informes para permitir mejoras del ROI. Con posibilidad de recibir un informe por centro.
  - Alineación del cumplimiento con el marco regulatorio.
- Revisión trimestral del sistema completo, emitiendo un informe sobre el estado de actualización de este y recomendaciones de actualización de versión y parches de seguridad, alineadas con las del fabricante.

En los informes de riesgos aparecerán las diversas acciones de mejora o propuestas priorizadas de remediación o mitigación según los problemas, riesgos o incidentes de seguridad detectados. El adjudicatario deberá tener en cuenta en la definición de estos procedimientos que serán tales que deberán facilitar la información que permita a la Comunidad de Madrid realizar las auditorías de seguridad y cumplimiento que considere necesarias (auditoría de accesos, tratamientos de datos de carácter personal, etc.) o valorar la calidad y seguridad de los servicios prestados y de los procedimientos de soporte remoto.

En situaciones excepcionales, como un ataque o explotación de vulnerabilidad, o de la indisponibilidad de la solución una vez implantada, el adjudicatario deberá tener definido el sistema de monitorización para que se puedan emitir informes de situación con la periodicidad requerida por la D.G. de Salud, que incluyan un resumen ejecutivo, cronología, sistemas de información afectados, perjuicio asistencial derivado, causa raíz del problema, estado de la investigación o remediación, plan de acción y recomendaciones.

El sistema de monitorización diseñado deberá tener que utilizar para la tramitación de incidencias, peticiones y consultas una herramienta de *ticketing* que la Dirección General de Salud Digital determine.

Asimismo, si para el sistema de monitorización diseñado y/o para cualquier actividad de administración del equipamiento desplegado en los centros hospitalarios o CPDs fuera preciso conectarse de forma remota a los equipos se ofrecerán dos alternativas, siendo todos los costes asociados por cuenta del adjudicatario en cualquiera de ellos:

- Instalación en los CPDs del SERMAS de unos equipos que proporcionan conectividad privada de nivel 3 con las instalaciones del adjudicatario. La Comunidad de Madrid cedería temporalmente un direccionamiento IP privado que debería presentarse en la red institucional de la Comunidad de Madrid para evitar colisiones de direccionamiento IP.

Cualquier posible colisión de las direcciones IP de los equipos instalados con la red del adjudicatario debería ser resuelta por el propio adjudicatario.

- Establecimiento de un túnel IPsec site-to-site a través de internet del adjudicatario hacia un terminador ubicado en los CPDs de la Comunidad de Madrid, bajo la política y parámetros de seguridad establecida para interconexiones por Madrid Digital y con las mismas consideraciones respecto al direccionamiento IP del caso anterior.

En caso de que durante el período de prueba del sistema de monitorización hiciera falta un acceso remoto VPN, éste debería ser proporcionado por el adjudicatario bajo un esquema obligatorio de doble factor de autenticación.

Por otro lado, con objeto de garantizar unos mínimos niveles de seguridad y cumplimiento en materia de seguridad de la información y las comunicaciones y de cumplimiento normativo, el adjudicatario deberá asumir determinadas obligaciones en aspectos de seguridad técnica, seguridad de la información y de protección de datos, durante todo el período de prueba (que se extenderá hasta la finalización de la última de las instalaciones) del sistema de monitorización diseñado:

En materia de seguridad técnica, el adjudicatario:

- Queda obligado a garantizar que cualquier dispositivo que deba conectarse a la red corporativa, tanto directamente como a través de sistemas o soluciones de acceso remoto, cumpla con los requisitos de seguridad siguientes:
  - Contar con un sistema operativo y software de base actualizado y con soporte del fabricante correspondiente. El adjudicatario asume el compromiso de actualizar el sistema y software de base a las correspondientes versiones que cuenten con soporte de los fabricantes a medida que dicho software vaya quedando fuera de soporte.
  - Mantener un nivel de actualizaciones razonable evitando exposiciones innecesarias y excesivas a vulnerabilidades software. En ningún caso se excederá de una ventana de aplicación de parches de seguridad de más de 4 meses desde la publicación del parche correspondiente, salvo que la organización, tras analizar los riesgos de llevar a cabo dicha actualización, decida lo contrario. Este nivel de seguridad se deberá mantener durante todo el ciclo de vida del software y para cualquier programa o software instalado en cualquier dispositivo que soporte al servicio y que esté conectado a la red de manera directa o a través de cualquier tipo de acceso remoto.
- Garantizará el cumplimiento de las medidas de seguridad de un sistema de categoría media de Esquema Nacional de Seguridad o equivalente. La organización se reserva la posibilidad de auditar dichas medidas de seguridad para lo cual contará con la colaboración del adjudicatario. Asimismo, el adjudicatario asumirá las obligaciones derivadas del cumplimiento del RDL 12/2018 de Seguridad de las redes y los sistemas de información, especialmente en lo relacionado a cooperación, notificación de incidentes y colaboración con las autoridades de supervisión y los CERT/CSIRT de referencia de las administraciones públicas, así como de cualquier otra obligación legal o normativa que deba asumir la D.G. Salud Digital y que, por tanto, deba extenderse al adjudicatario.
- Ajustará sus procedimientos y herramientas de soporte remoto a las herramientas, procedimientos y políticas de seguridad de Madrid Digital y del SERMAS.
- Colaborará con el Equipo de Respuesta ante Incidentes de seguridad de Madrid Digital y del SERMAS, en la respuesta ante cualquier incidente de ciberseguridad que pudiera comprometer la información o los servicios. En caso de que el incidente se produjera en los sistemas del adjudicatario, notificará inmediatamente este hecho al responsable del contrato y al responsable de Seguridad del SERMAS a través de los canales de comunicación establecidos para el seguimiento del contrato.

En materia de cumplimiento normativo:

Se asumirá el cumplimiento de las normas básicas de seguridad aprobadas por el SERMAS y Madrid Digital entre las que figuran la Política de Seguridad o la Política de Uso Aceptable de los Sistemas de Información en aquellos aspectos que afecten a proveedores de servicios y usuarios ocasionales de los sistemas de información y las redes de la Comunidad de Madrid.

## CLÁUSULA 5ª - -PLAZOS

El adjudicatario deberá ser capaz de desplegar los servicios en los siguientes plazos:

- **Reunión de lanzamiento:** Máximo 15 días tras la adjudicación del contrato. Determinará el comienzo del Periodo de Implantación.
- **Durante las 4 primeras semanas** del periodo de implantación de cada instalación el adjudicatario realizará una primera solicitud con objeto de recabar toda la información necesaria para las integraciones requeridas, así como identificar a los interlocutores responsables de aceptar las instalaciones
- **Mensualmente**, durante el periodo de Implantación, se realizará una reunión de seguimiento donde se analizará el ritmo de ejecución, la priorización de trabajos y se presentará un informe indicando el nivel de cumplimiento de los Acuerdos de Nivel de Servicio. Con una antelación de 48 horas a cada reunión mensual, el jefe de proyecto enviará un informe reflejando el estado de situación en cuanto a tareas realizadas, tareas pendientes e incidencias encontradas. La confección del acta y distribución de esta en un máximo de 2 días laborables será responsabilidad del jefe de proyecto del adjudicatario.
- El director técnico del proyecto por parte del adjudicatario o de la Comunidad de Madrid podrán solicitar, al margen de las reuniones establecidas la celebración de reuniones extraordinarias por la existencia de circunstancias que lo hagan necesario.
- **Instalación básica, configuración inicial, documentación y sesiones de traspaso de conocimiento básicas para el primer centro** realizadas 10 semanas desde la adjudicación del contrato.
- El proveedor entregará la **documentación final** de cada instalación en el plazo de una semana tras finalizar la instalación, para que los interlocutores nombrados por la Comunidad de Madrid procedan a la revisión y aceptación de la instalación.
- Durante la fase de implantación, el adjudicatario llevará a cabo una capacitación y gestión del cambio, que ayude a garantizar el éxito de la implantación de este nuevo sistema en un servicio de salud donde participan tan diversos perfiles. El Plan de Gestión del Cambio se deberá presentar para su aprobación por la Dirección General de Salud Digital antes de su ejecución, y debe incorporar como mínimo actividades que supongan 20 horas para personal de CPD y centros hospitalarios y 3 horas por cada centro de salud. Las sesiones de capacitación deberán haberse impartido antes del fin del periodo de implantación.

Los hitos de la siguiente tabla se considerarán cumplidos cuando se haya finalizado la implantación, que incluyen los suministros, las tareas de configuración básica e instalación inicial, independientemente de que los servicios de instalación avanzada deberán mantenerse hasta que se hayan completado todas las instalaciones asociadas al contrato y se hayan podido realizar las pruebas del conjunto del sistema. Los centros concretos que compondrán cada hito se definirán por la Dirección General de Salud Digital en la primera reunión mensual posterior a la de lanzamiento. De cara a su inclusión en los hitos, se entiende por centro cada uno de los 32 centros sanitarios incluidos en el alcance de este pliego, así como cada uno de los CPDs. En total, existen 34 centros cuyas implantaciones se reparten entre 4 hitos.

**La duración será de 15 meses o su fecha fin será hasta mayo de 2026, lo que antes se produzca.**

## Hitos y entregables

Hito	Descripción del hito y sus entregables	Plazo	Porcentaje de la prestación
<b>HITO_01</b>	<p>Finalización de la implantación en 9 hospitales</p> <p>Entregables:</p> <ul style="list-style-type: none"> <li>Guía de Operación, incluyendo la de las integraciones no asociadas a centros particulares</li> <li>Documentación de instalación de cada uno de los centros, incluyendo sus integraciones particulares</li> <li>Informe resumen de dispositivos detectados por tipología en cada uno de los centros</li> <li>Informe de vulnerabilidades y riesgos de cada uno de los centros, con priorización de los riesgos</li> </ul>	4 meses a partir del inicio de la ejecución	<p>28% de las licencias hospitalarias</p> <p>26% de los servicios de instalación avanzada y de la garantía extendida</p>
<b>HITO_02</b>	<p>Finalización de la implantación en 6 hospitales y dos CPDs</p> <p>Entregables:</p> <ul style="list-style-type: none"> <li>Guía de Operación</li> <li>Documentación de instalación de cada uno de los centros</li> <li>Informe resumen de dispositivos detectados por tipología en cada uno de los centros</li> <li>Informe de vulnerabilidades y riesgos de cada uno de los centros, con priorización de los riesgos</li> </ul>	4 meses después de la aceptación del HITO_01	<p>19% de las licencias hospitalarias 24% de los servicios de instalación avanzada y de la garantía extendida</p> <p>100% de las licencias de centros no hospitalarias</p>
<b>HITO_03</b>	<p>Finalización de la implantación en 8 hospitales</p> <p>Entregables:</p> <ul style="list-style-type: none"> <li>Guía de Operación</li> <li>Documentación de instalación de cada uno de los centros</li> <li>Informe resumen de dispositivos detectados por tipología en cada uno de los centros</li> <li>Informe de vulnerabilidades y riesgos de cada uno de los centros, con priorización de los riesgos</li> </ul>	3 meses después de la aceptación del HITO_02	25% de las licencias hospitalarias 24% de los servicios de instalación avanzada y de la garantía extendida
<b>HITO_04</b>	<p>Finalización de la implantación en 9 hospitales</p> <p>Entregables:</p> <ul style="list-style-type: none"> <li>Guía de Operación</li> <li>Documentación de instalación de cada uno de los centros</li> <li>Informe resumen de dispositivos detectados por tipología en cada uno de los centros</li> <li>Informe de vulnerabilidades y riesgos de cada uno de los centros, con priorización de los riesgos</li> </ul>	4 meses después de la aceptación del HITO_03	28% de las licencias hospitalarias 26% de los servicios de instalación avanzada y de la garantía extendida



## CLÁUSULA 6ª - RECURSOS APORTADOS POR EL ADJUDICATARIO

El adjudicatario deberá de poner a disposición del contrato un **responsable del Proyecto**. Dicho responsable de Proyecto será el interlocutor principal para todos los aspectos técnicos y económicos relativos al proyecto.

Para llevar a cabo los servicios necesarios se estiman, como mínimo, al menos los siguientes roles:

SERVICIOS	Horas
Jefe de Proyecto	760
Consultor Senior	380
Técnico de Sistemas/Integraciones	3.635
Analista	3.680
<b>Total Servicios</b>	<b>8.455</b>

### Funciones Perfiles

Jefe de proyecto: Función de coordinación técnica del proyecto. Responsabilidad de la organización, del desarrollo y control permanente del proyecto. Desarrollo del plan de trabajo y elaboración de los informes periódicos de avance.

Consultor senior: Análisis de las necesidades del sistema. Elaboración del diseño técnico global. Interacción en las capturas de requisitos, definición de impacto de los requisitos y diseño de las soluciones a implementar.

Técnico de Sistemas/Integraciones: Ejecución y verificación entre sistemas y de migración.

Analista: Identificar los requisitos planteados por el consultor y definir el diseño de los componentes a desarrollar, de tal forma que el programador pueda diseñar, programar y testear el sistema.

### Experiencia y titulación de perfiles

A continuación, se indican los requisitos esenciales en cuanto a la experiencia de perfiles.

EXPERIENCIA/FORMACION REQUERIDA DE CADA PERFIL
<b>Jefe de Proyecto</b>
<ul style="list-style-type: none"><li>- Titulación universitaria en estudios relacionados.</li><li>- 4 años en gestión de proyectos ligados a entornos sanitarios o de Ciberseguridad.</li></ul>
<b>Consultor</b>
<ul style="list-style-type: none"><li>- Titulación universitaria en estudios relacionados.</li><li>- 3 años en gestión de proyectos ligados a entornos sanitarios o de Ciberseguridad.</li></ul>
<b>Técnico de Sistemas/Integraciones</b>
<ul style="list-style-type: none"><li>- Titulación universitaria o Formación profesional en estudios relacionados.</li><li>- Al menos 3 años en proyectos ligados a entornos sanitarios o de Ciberseguridad.</li></ul>
<b>Analista</b>
<ul style="list-style-type: none"><li>- Titulación universitaria o Formación profesional en estudios relacionados.</li><li>- 2 años en proyectos ligados a entornos sanitarios o de Ciberseguridad.</li></ul>

## CLÁUSULA 7ª - ACUERDOS DE NIVEL DE SERVICIO

A efectos de cálculo del cumplimiento de los ANS, sólo computa el tiempo transcurrido dentro del horario de prestación del servicio descrito en apartados anteriores.

Id.	Nombre	Descripción del indicador	Valor
ANS_01	Tiempo de respuesta	Durante el periodo de pruebas del sistema de monitorización, el tiempo transcurrido desde la comunicación de la incidencia hasta que el equipo comunica que ha empezado a trabajar en su resolución no debe superar el valor indicado.	2 horas en horario de atención
ANS_02	Tiempo de resolución de incidencia leve	Tiempo transcurrido desde el final del tiempo de respuesta hasta que el equipo ha solucionado la incidencia.	8 horas laborables
ANS_03	Tiempo de resolución de incidencia grave	No incluye el tiempo necesario para la aprobación por el responsable del Contrato Específico.	4 horas laborables
ANS_04	Tiempo de resolución de incidencia crítica		4 horas laborables
ANS_05	Detección automática en la fase de implantación	El sistema deberá clasificar por naturaleza automáticamente la tasa de equipos indicada. No se considerarán como detectados automáticamente aquellos equipos que queden clasificados en categorías genéricas como "Otros", "Desconocido" u otra de significado equivalente.	80% de los equipos conectados a la red
ANS_06	Tasa de equipos clasificados de forma genérica al finalizar la fase de implantación	Los trabajos de implantación en un hospital nunca se considerarán como finalizados mientras exista una tasa superior a la indicada de equipos clasificados por naturaleza en una categoría genérica para las redes dependientes de ese hospital. No será de aplicación para centros de salud o de especialidades	5% de los equipos conectados a la red
ANS_07	Entrega de informes mensuales	Retraso en el nº de informes mensuales indicados en cualquier fase del proyecto	1

De cara a los Acuerdos de Nivel de Servicio:

- Un fallo en la entrega de datos de una colectora se considera incidencia crítica.
- En caso de que el fallo se produzca en un equipo instalado en un centro, y la solución requiera de un reemplazo hardware, el ANS de resolución de incidencia crítica finaliza con la petición del reemplazo al fabricante.
- El reemplazo del fabricante y resolución definitiva de la incidencia crítica deberá estar finalizado al término del siguiente día laborable. El equipo, su envío, sustitución del equipo averiado, y retirada del mismo, son por cuenta del adjudicatario.
- Se considera incidente crítico si la plataforma se encuentra inoperativa, incide en la red del SERMAS, o en la prestación de sus servicios. Igualmente, la falta de localización de un dispositivo conectado a la red que cause idénticos efectos.
- Se considera incidente grave si hay una funcionalidad básica concreta del producto no operativa en un centro sin una remediación conocida o aplicable en un corto espacio de tiempo.

Cuando la resolución de la incidencia requiera la realización de desarrollos que por su naturaleza necesitan de un plazo material superior al indicado en la tabla precedente, el contratista estará



obligado a presentar al Responsable del Contrato Específico en el organismo destinatario, dentro del plazo de tiempo de resolución inicial, un plan de actuación que incluya la duración prevista de los trabajos para la resolución, la justificación de dicha previsión y la descripción de los trabajos a realizar. Si es necesario, se incluirá la descripción de las medidas paliativas a adoptar hasta la completa resolución de la incidencia. Dicho plan deberá ser aprobado por el responsable del Contrato Específico.

## INFORMACIÓN REQUERIDA UNIÓN EUROPEA FONDO MRR

### 1. INTRODUCCIÓN

La presente licitación se encuadra en el marco del Plan de Recuperación, Transformación y Resiliencia, dentro del eje transversal de transformación digital, en la política palanca IV “IV. Una Administración para el Siglo XXI”, se encuadra el Componente 11i03 “Modernización de las Administraciones Públicas”

Dicho Componente, tiene por objetivo la modernización del conjunto de agentes del sector público, mediante su digitalización, la renovación de su equipamiento con principios de eficiencia energética, y la modernización de procesos, además de la capacitación del conjunto de empleados públicos, todos ellos objetivos importantes del Plan de Recuperación, Transformación y Resiliencia, recogidos de forma transversal en el mismo y de forma específica en el presente componente.

Dentro del Componente 11, se incluye la Línea 6 Sanidad. La transformación digital del sistema nacional de salud constituye el núcleo de la medida 34 del eje 7 de la Agenda España Digital 2025 que incorpora, entre otras acciones la de “favorecer una atención personalizada a las necesidades de la ciudadanía”.

En esa dirección, dentro del PERTE “Salud de Vanguardia” asociado al objetivo 4 (“Impulsar la transformación digital de la asistencia sanitaria, mediante la aplicación de tecnología a todas las actividades que impliquen relación con la ciudadanía y de gestión de los recursos en todos los ámbitos asistenciales, con particular atención al refuerzo de la atención primaria y a la equidad en el acceso a una atención sanitaria de calidad, en condiciones de ciberseguridad”) la línea 6 de la inversión 3 del componente 11 se ha dedicado al Plan de Transformación Digital de la Atención Primaria y comunitaria.

Como extensión y ampliación de este Plan y apoyándose en sus resultados, se desarrollará el Plan de Atención Digital personalizada, para crear en el SNS un apoyo tecnológico para la implantación de estos servicios que se aplicará de manera coordinada y continuada a través de todos los niveles asistenciales, más allá de la atención primaria y comunitaria.

Dentro del citado componente 11, se establecen los siguientes hitos y objetivos:

- se define el Hito CID 169 como la “finalización de todos los proyectos del Plan de Atención Digital Personalizada” (segundo trimestre de 2026)

### 2. OBJETO DEL CONTRATO

El objeto de este contrato es establecer los requisitos técnicos mínimos que han de regir los servicios de suministro, configuración e instalación avanzada de un sistema de control y seguridad de los equipos conectados a la red de comunicaciones de los centros de Atención Primaria del SERMAS, que se describe en el apartado 3 y 4 de este PPT.

### 3. PRINCIPIO DNSH (ARTÍCULO 5 ORDEN HFP/1030/2021)

La empresa adjudicataria deberá respetar los principios de economía circular y evitar impactos negativos en el medio ambiente (DNSH, por sus siglas en inglés, “do no significant harm”) en la ejecución de las actuaciones llevadas a cabo en el marco del PRTR.

#### 4. ETIQUETADO VERDE Y ETIQUETADO DIGITAL (ARTÍCULO 4 ORDEN HFP/1030/2021)

El contratista estará obligado al preceptivo cumplimiento de las obligaciones asumidas en materia de etiquetado verde y etiquetado digital y los mecanismos establecidos para su control, así como al preceptivo cumplimiento de las obligaciones asumidas por la aplicación del principio de no causar un daño significativo y las consecuencias en caso de incumplimiento.

El Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo de 12 de febrero de 2021 por el que se establece el Mecanismo de Recuperación y Resiliencia, establece en sus Anexos VI y VII la Metodología de seguimiento para la acción por el clima y la metodología para el etiquetado digital en el marco del Mecanismo, respectivamente.

El Plan de Recuperación, Transformación y Resiliencia, en su componente 11, Inversión 3, y en aplicación del Reglamento (UE) 2021/241, recoge que la contribución a la transición ecológica de este componente es de un 0% y a la transición digital de un 100%.

El contrato en tramitación corresponde a la ejecución de la inversión C11.I03, por lo que la contribución a los objetivos de transición ecológica y digital será de un 0% y 100% respectivamente. Con el objetivo de facilitar el seguimiento y evaluación del cumplimiento del compromiso de etiquetado verde y digital, se incorporará al sistema de información y seguimiento la aportación del subproyecto indicado al objetivo fijado.


#### 5. OBLIGACIONES DEL CONTRATISTA: INFORMES DE EJECUCIÓN Y REPORTE DE INFORMACIÓN

El contratista tendrá las siguientes obligaciones relativas a los Informes de ejecución y reporte de otra información:

- Deberá informar a la Dirección General promotora del contrato, proactivamente, sobre cualquier evento importante o imprevisto que pueda impactar en la consecución de los objetivos establecidos.
- Establecerá mecanismos de reporte y ejecución de los fondos.
- Durante la ejecución del contrato, en su caso, se establecerán mecanismos de reporte del cumplimiento de los principios de publicidad y comunicación.
- Deberá informar con inmediatez de la existencia de cualquier procedimiento judicial tendente a la determinación de conductas que puedan ser constitutivas de infracción penal y que afecten a las actuaciones financiadas total o parcialmente con cargo a estas subvenciones, así como de cualquier otra incidencia que pueda perjudicar a la reputación del Mecanismo de Recuperación y Resiliencia.

#### EL TITULAR DEL ÓRGANO DESTINATARIO (CARGO):

DIRECTORA GENERAL DE SALUD DIGITAL.

Firmado digitalmente por: NURIA RUIZ HOMBREBUENO -   
Fecha: 2024.11.28 14:49

Firmado electrónicamente (nombre y apellidos): Nuria Ruiz Hombrebueno.