ACTA DE LA CELEBRACIÓN DE LA SESIÓN SOBRE LA DEMOSTRACIÓN RELATIVA A LA VERIFICACIÓN DEL EFECTIVO CUMPLIMIENTO DE LOS REQUISITOS MÍNIMOS ESPECIFICADOS EN EL PLIEGO DE PRESCRIPCIONES TÉCNICAS Y, EN SU CASO, LOS VALORES OFERTADOS EN RELACIÓN CON EL CRITERIO DE ADJUDICACIÓN N.º 2 "FUNCIONALIDADES ADICIONALES" DE LA SOLUCIÓN OFERTADA AL EXPEDIENTE 2120/2025 "CONTRATACIÓN DE LA SUSCRIPCIÓN A UNA SOLUCIÓN PARA LA MONITORIZACIÓN DEL EQUIPAMIENTO MÉDICO CONECTADO DEL SERVICIO ANDALUZ DE SALUD Y SU INSTALACIÓN, COFINANCIADO CON FONDOS DEL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA (MRR) DESTINADOS A PROYECTOS ESTRATÉGICOS PARA LA RECUPERACIÓN Y TRANSFORMACIÓN ECONÓMICA (PERTE)", POR LA PERSONA LICITADORA "BABEL SISTEMAS DE INFORMACIÓN, S.L.U."

En Sevilla, siendo las 8:00 a.m. del día 15 de mayo de 2026 se celebra, de forma telemática, reunión técnica con objeto de verificar el efectivo cumplimiento de los requisitos mínimos, según lo especificado en el apartado "Requisitos técnicos del producto" del Pliego de Prescripciones Técnicas, así como de los valores ofertados en relación con el criterio de adjudicación n.º 2 "Funcionalidades Adicionales", de la solución ofertada por la persona licitadora BABEL SISTEMAS DE INFORMACIÓN, S.L.U. en relación al expediente 2120/2025 "CONTRATACIÓN DE LA SUSCRIPCIÓN A UNA SOLUCIÓN PARA LA MONITORIZACIÓN DEL EQUIPAMIENTO MÉDICO CONECTADO DEL SERVICIO ANDALUZ DE SALUD Y SU INSTALACIÓN, COFINANCIADO CON FONDOS DEL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA (MRR) DESTINADOS A PROYECTOS ESTRATÉGICOS PARA LA RECUPERACIÓN Y TRANSFORMACIÓN ECONÓMICA (PERTE)", según lo establecido en el apartado 16.2 del Cuadro Resumen del Pliego de Cláusulas Administrativas Particulares.

La presente sesión se desarrolla conforme al procedimiento establecido en el citado apartado 16.2 del Cuadro Resumen del PCAP, habiendo sido requerida para ello la persona licitadora que obtuvo la mayor puntuación tras la valoración de los criterios de adjudicación. Asimismo, la demostración se realiza en entorno habilitado por la persona licitadora, reproduciendo la solución ofertada y poniendo a disposición del Servicio Andaluz de Salud los medios necesarios para efectuar las tareas de validación técnica correspondientes.

Asisten a la reunión las personas que se detallan a continuación:

- En representación del Servicio Andaluz de Salud (SAS):
  - Manuel Jimber del Río
  - Alfonso Orellana Muñoz
- En representación de BABEL SISTEMAS DE INFORMACIÓN, S.L.U:
  - Antonio Marín Pastor

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	MANUEL JIMBER RIO	15/05/2026
	ALFONSO ORELLANA MUÑOZ	
VERIFICACIÓN	Pk2jmX8D9HQNVBMJ4XHMP8M6URVB5K	PÁG. 1/7

1. Verificación del efectivo cumplimiento de los requisitos técnicos establecidos como mínimos en el Pliego de Prescripciones Técnicas (PPT)

Se comienza por la verificación, mediante un conjunto de exámenes y preguntas, de los requisitos técnicos establecidos como mínimos en el Pliego de Prescripciones Técnicas (PPT), siendo el resultado de dicha verificación el siguiente:

REQUISITO TÉCNICO DE LA SOLUCIÓN	DESCRIPCIÓN	CUMPLE
REQ 1.	La solución debe estar diseñada de forma que la detección del equipamiento sea mediante sondas físicas instaladas localmente en cada centro.	SÍ
REQ 2.	La solución debe monitorizar los dispositivos de Internet of Medical Things (IoMT), Internet of Things (IoT), Operational Technology (OT) e Information Technology (IT).	SÍ
REQ 3.	La gestión de la solución será desde un navegador Web (consola de gestión) y no requerirá la instalación de ningún tipo de aplicación para su uso.	SÍ
REQ 4.	La consola de gestión se ofrecerá como un servicio SaaS hospedado en un Data Center en la Unión Europea cuyo proveedor cuente con la certificación en nivel alto del Esquema Nacional de Seguridad.	SÍ
REQ 5.	La consola de gestión deberá ofrecerse, al menos, en idioma inglés.	SÍ
REQ 6.	La consola de gestión será multisite y deberá permitir la creación de usuarios con diferentes roles y alcances, pudiendo configurarse la visibilidad de éstos limitándola al equipamiento que se encuentra dentro de su ámbito de responsabilidad. Se garantizará la separación de la información por cada sede del SAS y la gestión completa desde una sede principal.	SÍ
REQ 7.	La solución deberá gestionar un sistema multiusuario que facilite realizar perfilado de usuarios según módulos/funciones. Al menos, se deberán poder asignar a los diferentes interesados los siguientes permisos categorizados: • Para técnicos de ciberseguridad, con acceso a vulnerabilidades, riesgos, sugerencias de mitigación y cualquier información necesaria para su trabajo. • Para personal de electromedicina, que permita acceder a los datos de uso de los distintos dispositivos. • De gestión de inventario, para acceder a los datos que permitan mantener el inventario de la organización. • De configuración, para técnicos de ciberseguridad que puedan configurar la solución.	SÍ
REQ 8.	La solución deberá permitir el acceso a todos los módulos a los que tenga permiso desde una misma sesión, sin que requiera del usuario múltiples autentificaciones.	SÍ

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	MANUEL JIMBER RIO	15/05/2026
	ALFONSO ORELLANA MUÑOZ	
VERIFICACIÓN	Pk2jmX8D9HQNVBMJ4XHMP8M6URVB5K	PÁG. 2/7

REQUISITO TÉCNICO DE LA SOLUCIÓN	DESCRIPCIÓN	CUMPLE
REQ 9.	La solución propuesta debe ser totalmente pasiva en la monitorización, realizándose esta monitorización mediante sondas o colectores que serán elementos hardware que se instalarán localmente en cada ubicación que analicen el tráfico de este equipamiento. La solución debe operar sin impacto en los sistemas finales.	SÍ
REQ 10.	La solución no debe requerir la instalación de agentes en los equipos a monitorizar para las funcionalidades obligatorias expresadas en el presente PPT.	SÍ
REQ 11.	Las sondas o colectores, además de la instalación hardware exigida, deben poder desplegarse en formato virtual.	SÍ
REQ 12.	Las sondas o colectores serán nuevos. No se admitirán elementos de segunda mano o reacondicionados.	SÍ
REQ 13.	Las sondas o colectores deben contar con las siguientes características: - 1U o 2U, según el resultado del estudio previo de instalación realizado en cada centro. - Para administración y gestión, al menos 1 enlace de cobre o fibra a 1Gb. - Para administración fuera de banda, al menos 1 enlace de cobre o fibra a 1Gb. - Para captura de tráfico, al menos 1 enlace de fibra y 1 de cobre a 10 Gb. - Doble fuente de alimentación con PDU. El adjudicatario deberá proveer cualquier conector, cable y pequeño material y convertidor de medio que sea necesario para la conectividad de las sondas o colectores.	SÍ
REQ 14.	La solución incluirá la instalación de TAPs (Test Access Point) a los que irán conectadas las sondas. Estos permitirán replicar el tráfico del puerto al que se conecte. El TAP será de fibra o cobre, según las necesidades de la ubicación concreta, con capacidades de 10Gbps. Se dejará conectado al TAP el nuevo equipamiento y el ya existente (de haberlo) dejando, al menos, otro puerto para futuras necesidades del servicio.	SÍ
REQ 15.	La solución deberá contar con funcionalidades de descubrimiento, identificación, inventariado y perfilado del equipamiento conectado a la red cableada y Wifi. Hará uso de Deep Packet Inspection (Análisis profundo de paquetes) y clasificará los dispositivos IoMT, IoT, IT y OT de una manera determinista.	SÍ
REQ 16.	La solución incluirá un inventario en vivo y siempre actualizado de activos médicos conectados.	SÍ
REQ 17.	La solución incluirá una vista centralizada del inventario de activos que permita filtrar, crear búsquedas guardadas, crear informes.	SÍ

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	MANUEL JIMBER RIO	15/05/2026
	ALFONSO ORELLANA MUÑOZ	
VERIFICACIÓN	Pk2jmX8D9HQNVBMJ4XHMP8M6URVB5K	PÁG. 3/7

REQUISITO TÉCNICO DE LA SOLUCIÓN	DESCRIPCIÓN	CUMPLE
REQ 18.	La solución mostrará información de cada dispositivo detectado y posibilitará su incorporación al inventario corporativo mediante un interfaz de integración. Para el caso de los dispositivos médicos, esta información no será genérica y beberá de una base de datos con información específica de dispositivos médicos.	SÍ
REQ 19.	La solución debe ser capaz de detectar e identificar equipamiento IoMT conectado a la red Ethernet por adaptadores/conversores de puerto serie.	SÍ
REQ 20.	La solución realizará análisis de riesgos y vulnerabilidades para todos los tipos de dispositivos médicos.	SÍ
REQ 21.	Los datos usados por la solución estarán basados en la información que pueda recoger de forma pasiva y cruzar con Bases de Datos de vulnerabilidades, sin lanzar análisis de vulnerabilidades activos que impacten sobre el servicio del equipamiento.	SÍ
REQ 22.	La solución debe categorizar las amenazas y proponer protocolos de actuación según su tipología.	SÍ
REQ 23.	La solución deberá disponer de capacidad de retención y análisis de los eventos y tráfico detectado. La capacidad de retención de eventos será, al menos, de 90 días.	SÍ
REQ 24.	La solución debe monitorizar y analizar todos los flujos de tráfico de red en tiempo real. El que entra y sale del entorno de red y el que se mueve lateralmente a través de la red.	SÍ
REQ 25.	La solución propuesta deberá representar un mapa de comunicaciones global y por dispositivos identificando su ubicación física.	SÍ
REQ 26.	La solución deberá añadir información de contexto proveniente de una base de datos propia de los atributos disponibles para los dispositivos detectados.	SÍ
REQ 27.	La solución debe contar con la capacidad de distinguir entre dispositivos inventariados y no inventariados (nuevos dispositivos).	SÍ
REQ 28.	La solución debe permitir la identificación, manual o mediante algún procedimiento establecido, de los equipos desconocidos o que la propia solución no sea capaz de identificar de forma correcta.	SÍ
REQ 29.	La solución debe permitir programar informes mensuales diferenciados por centros y por tipos de usuarios finales.	SÍ
REQ 30.	La solución deberá disponer, al menos, de capacidad de integración con sistemas y servicios corporativos vía API y a nivel L2 y L3 tales como: DHCP, SNMP, Gestión de red, Firewall, SIEM, Sistema Antimalware, Sistemas de detección de vulnerabilidades, sistemas de control de acceso NAC y herramientas de Ticketing.	SÍ

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	MANUEL JIMBER RIO	15/05/2026
	ALFONSO ORELLANA MUÑOZ	
VERIFICACIÓN	Pk2jmX8D9HQNVBMJ4XHMP8M6URVB5K	PÁG. 4/7

REQUISITO TÉCNICO DE LA SOLUCIÓN	DESCRIPCIÓN	CUMPLE
REQ 31.	La solución debe incluir representaciones de las VLANs que indiquen los tipos de dispositivos que se conectan con información detallada de cada uno de ellos separados por VLAN.	SÍ
REQ 32.	La solución incluirá interfaces que describan la comunicación y el intercambio de información entre distintos tipos de dispositivos. Ésta se ofrecerá mediante representaciones gráficas que permitan identificar con facilidad comunicaciones anómalas entre dispositivos o con el exterior.	SÍ
REQ 33.	La solución debe poder generar informes de cumplimiento normativo.	SÍ
REQ 34.	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 Andaluz de Salud.	SÍ
REQ 35.	La solución debe proporcionar a los analistas del centro de operaciones de seguridad (SOC en sus siglas en inglés) información sobre la postura de seguridad actual y los riesgos y amenazas a la infraestructura.	SÍ
REQ 36.	La solución será capaz de mostrar en la misma consola de gestión información sobre las pruebas médicas que realizan los distintos dispositivos, no incluyendo datos de pacientes.	SÍ
REQ 37.	La solución dispondrá de interfaces que permitan interpretar con facilidad los datos de uso de los dispositivos por parte de personal no informático. Los datos de uso detallarán tipos de pruebas médicas específicas realizadas, numero de estas, uso en distintos horarios y se presentarán en interfaces usables por los perfiles de gestión de las áreas clínicas.	SÍ
REQ 38.	En la solución, los datos en tránsito y los datos en reposo deben estar cifrados en todo momento.	SÍ
REQ 39.	La solución debe incluir los formularios MDS2 de los dispositivos que detecta.	SÍ
REQ 40.	Los datos MDS2 se deben poder utilizar para crear informes y alertas en la solución.	SÍ
REQ 41.	La solución debe realizar detección de ataques en tiempo real.	SÍ
REQ 42.	La solución no debe almacenar datos de salud ni personales.	SÍ
REQ 43.	La solución debe ser capaz de evaluar automáticamente los dispositivos en busca de vulnerabilidades, exposición a amenazas, problemas de red y problemas operativos.	SÍ
REQ 44.	La solución tiene que actualizar automáticamente el estado del riesgo. Los riesgos que se mitigaron se marcarán como Mitigados (detectados automáticamente) o Inactivos, en caso de que el riesgo no se haya observado en la conexión durante un período de tiempo.	SÍ
REQ 45.	La solución proporcionará un plan de mitigación basado en los riesgos.	SÍ
REQ 46.	La solución debe recomendar políticas de segmentación.	SÍ

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	MANUEL JIMBER RIO	15/05/2026
	ALFONSO ORELLANA MUÑOZ	
VERIFICACIÓN	Pk2jmX8D9HQNVBMJ4XHMP8M6URVB5K	PÁG. 5/7

Los representantes del SAS certifican que la persona licitadora **cumple** con todos los requisitos establecidos como mínimos en el Pliego de Prescripciones Técnicas (PPT), continuándose con el procedimiento de demostración con la verificación del cumplimiento de los requisitos establecidos en el criterio de adjudicación n.º 2 Funcionalidades adicionales.

2. Verificación del efectivo cumplimiento de los valores ofertados en relación con el criterio de adjudicación n.º 2 "Funcionalidades adicionales"

Se detallan las características técnicas y funcionales adicionales de la solución ofertada y el resultado de la verificación:

FUNCIONALIDAD ADICIONAL	DESCRIPCIÓN	OFERTADO	CUMPLE
FA 1.	La solución incluye la capacidad de dar acceso remoto a los dispositivos IoMT o IoT monitorizados por la solución, permitiendo otorgar diferentes privilegios al usuario. La sesión se podrá grabar o ver en directo, se podrá bloquear en cualquier momento y se podrá gestionar la autorización del acceso del usuario por los administradores designados para ello.	SÍ	SÍ
FA 2.	La solución dispondrá, mediante la ejecución de un módulo al efecto, de una aplicación que permite obtener información de las zonas aisladas del resto de la red o de zonas donde no tenga acceso. Se incluirá con la solución de forma nativa y se podrá usar de forma complementaria al resto de métodos de identificación.	SÍ	SÍ
FA 3.	La solución es capaz de sincronizar políticas y objetos de políticas a través de la integración con las herramientas existentes en el SAS (NAC, firewall).	SÍ	SÍ
FA 4.	La solución realiza un Análisis de IA de los flujos de tráfico médico para detectar nuevas vulnerabilidades y ataques Zero-day.	SÍ	SÍ
FA 5.	La consola de gestión se ofrece en idioma castellano.	SÍ	SÍ
FA 6.	La solución alerta sobre nuevos dispositivos conectados a la red	SÍ	SÍ
FA 7.	Las sondas o colectores tienen un modo pass-through que permite la conexión de otro dispositivo en cascada.	SÍ	SÍ
FA 8.	La solución identifica los elementos monitorizados a los que se accede con credenciales predeterminadas, débiles y/o compartidas.	SÍ	SÍ
FA 9.	La solución identifica los avisos de retirada que afectan a los dispositivos.	SÍ	SÍ

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	MANUEL JIMBER RIO	15/05/2026
	ALFONSO ORELLANA MUÑOZ	
VERIFICACIÓN	Pk2jmX8D9HQNVBMJ4XHMP8M6URVB5K	PÁG. 6/7

FUNCIONALIDAD ADICIONAL	DESCRIPCIÓN	OFERTADO	CUMPLE
FA 10.	Las comunicaciones salientes por Internet de los dispositivos monitorizados que transportan información médica se marcan e identifican específicamente.	SÍ	SÍ
FA 11.	La solución se integra con la base de datos de GMAO para proporcionar un inventario preciso de los activos	SÍ	SÍ
FA 12.	La solución dispone de una integración con el software de CrowdStrike que permite enriquecer el inventario de dispositivos de CrowdStrike Falcon con los activos detectados por la solución, aportando contexto de riesgo y vulnerabilidades para mejorar la gestión y priorización de amenazas en CrowdStrike Falcon.	SÍ	SÍ
FA 13.	La solución tiene integraciones con soluciones NAC en las que se inyecta la información de los dispositivos detectados.	SÍ	SÍ

Los representantes del SAS certifican que la persona licitadora **cumple** con todos los requisitos establecidos en el criterio de adjudicación n.º 2 Funcionalidades adicionales y que los valores ofertados en dicho criterio se corresponden con el resultado de la prueba realizada.

Conclusiones

A la vista de las verificaciones y comprobaciones efectuadas durante la presente sesión, se considera validada la demostración realizada por la persona licitadora BABEL SISTEMAS DE INFORMACIÓN, S.L.U., de conformidad con lo establecido en el apartado 16.2 del Cuadro Resumen del PCAP, considerándose definitiva la baremación previamente obtenida respecto de los extremos objeto de validación, elevando este resultado a la mesa de contratación.

Y no habiendo más asuntos que tratar, se levanta la sesión siendo las 09:30 horas del día indicado.

En representación del SAS

El representante de la empresa

BABEL

Firmado digitalmente por 48960144K ANTONIO MARIN (R: B83603191)
Fecha: 2026.05.15 09:45:32 +02'00'

Fdo.: Manuel Jimber del Río Fdo.: Alfonso Orellana Muñoz Fdo.: Antonio Marín Pastor

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	MANUEL JIMBER RIO	15/05/2026
	ALFONSO ORELLANA MUÑOZ	
VERIFICACIÓN	Pk2jmX8D9HQNVBMJ4XHMP8M6URVB5K	PÁG. 7/7