Suministro, instalación y mantenimiento de una Infraestructura de Seguridad en Centros de Osakidetza – Plan de Recuperación, Transformación y Resiliencia – Financiado por la Unión Europea – NextGenerationEU

Especificaciones de compra / Pliego de condiciones técnicas

Abril 2023

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia

EUSKO JAURLARITZA GOBIERNO VASCO

UNICO SERVICIOS PÚBLICOS

Mediterráneo, 14 • 01010 Vitoria-Gasteiz • Tel. 945 01 73 00* • www.ejie.eus

Este documento es propiedad de Eusko Jaurlaritzaren Informatika Elkartea – Sociedad Informática del Gobierno Vasco, S.A. (EJIE). Este documento no puede ser reproducido, en su totalidad o parcialmente, ni mostrado a otros, ni utilizado para otros propósitos que los que han originado su entrega, sin el previo permiso escrito de EJIE. En el caso de ser entregado en virtud de un contrato, su utilización estará limitada a lo expresamente autorizado en dicho contrato. EJIE no podrá ser considerada responsable de eventuales errores u omisiones en la edición del documento.

Versión	Fecha	Resumen de cambios	Elaborado por:	Aprobado por:
1.0	03/04/2023	Versión Inicial	Josu Bagazgoitia Séz de Vicuña	Aritza Iratzagorria Garay

Índice

1 Introducción 5

1.1 Perfil de la Compañía 5
1.2 Antecedentes 7

2 Objeto y Alcance del contrato 8

2.1 Objeto de la Contratación 8
2.2 Alcance de la Contratación 8
2.3 Descripción de Situación 9
2.3.1 Seguridad Dispositivos 9
2.3.2 Roadmap Seguridad Dispositivos. 9
2.3.3 Información de Contexto 9
2.4 Modelo de Servicio 10
2.4.1 Alcance del Servicio 10
2.4.2 Periodo de Prestación del Servicio 13

3 Requisitos técnicos y funcionales 14

3.1 Requisitos Diseño de la Solución 14
3.2 Requisitos Firewalls Centros 16
3.2.1 Modelos y Cantidad 16
3.2.2 Hardware 17
3.2.3 Funcionalidades 18
3.3 Requisitos Gestión, Logs y Reporting centralizado 20
3.4 Checklist de requerimientos 21

4 Servicios Profesionales 22

4.1 Servicios de Puesta en Marcha 22
4.1.1 Servicios de consultoría y diseño de la solución 23
4.1.2 Plan de actuación en los centros sanitarios. 23
4.1.3 Servicios de instalación, configuración y puesta en marcha 25
4.1.4 Otros servicios de definición previos al despliegue 26
4.1.5 Documentación 27
4.1.6 Transferencia de conocimiento 29
4.1.7 Recepción provisional de las instalaciones en centros 30
4.1.8 Operación y Explotación 31
4.2 Servicios de Ajuste y acondicionamiento del servicio 31
4.3 Servicios de Mantenimiento (Nivel 3) 32
4.3.1 Servicio de Mantenimiento Correctivo 33
4.3.2 Servicio de Mantenimiento Preventivo 35
4.3.3 Servicios de Mantenimiento Adicionales de Tercer Nivel del Adjudicatario 36
4.3.4 Otros Requisitos Asociados a la Prestación del Servicio de Mantenimiento 37
4.3.5 Problemáticas de rendimiento y/o funcionamiento identificadas durante el período de vigencia del contrato 38
4.3.6 Garantía, soporte y mantenimiento 38
4.4 Requisitos asociados a los servicios 39

4.4.1 Plazos Parciales de Ejecución 39
4.4.2 Requisitos Generales 40
4.4.3 Seguimiento y control de la ejecución del proyecto 41
4.4.4 Coordinación global del proyecto 41
4.4.5 Control de ejecución por parte del adjudicatario 42
4.4.6 Gestión documental 43
4.4.7 Reuniones de seguimiento 44
4.5 Equipo de trabajo 44
5 Anexos 47
5.1 Anexo I PCT_Checklist requisitos técnicos 47

1 Introducción

1.1 Perfil de la Compañía

EJIE, Eusko Jaurlaritzaren Informatika Elkartea – Sociedad Informática del Gobierno Vasco, es la Empresa pública de servicios de las tecnologías de la información y las comunicaciones (TIC), cuya razón de existir es contribuir a la consecución de un Sector Público Vasco, moderno y eficiente, en el Marco Legal establecido por el Gobierno, con la seguridad y calidad necesarias y con el debido respeto al medio ambiente.

EJIE tiene como meta final la consecución de la satisfacción de sus clientes, siendo el instrumento común de prestación de servicios TIC en el Sector Público Vasco, y comprometiéndose en:

- Construir y mantener con eficiencia y calidad la infraestructura de los Sistemas de Información, posibilitando su continuidad y seguridad.
- Garantizar la interoperabilidad entre las distintas administraciones.
- Servir de apoyo a las necesidades de planificación y realización de la función informática de los Departamentos y Organismos Autónomos del Gobierno, asegurando la cobertura de sus demandas con el compromiso y profesionalidad adecuados a las relaciones contractuales que se establezcan.

Por tanto, EJIE debe ser, un instrumento común de referencia para la prestación de servicios TIC en el Sector Público Vasco:

  - Aportando valor añadido.
  - Proporcionando soluciones competitivas.
  - Transmitiendo confianza a sus clientes.
  - Contando con personas cualificadas y comprometidas.

Se puede obtener información más detallada y extensa en nuestra dirección de Internet http://www.ejie.eus.

Con fecha 16 de agosto de 2016 se firmó el Acuerdo entre el Ente Público de Derecho Privado Osakidetza y Eusko Jaurlaritzaren Informatika Elkartea—Sociedad Informática del Gobierno Vasco, S.A. (EJIE) para la integración del servicio de infraestructuras y operaciones (I.O.) de OSAKIDETZA con el análogo servicio (I.O.) en EJIE, en el marco del acuerdo adoptado por el Consejo de Gobierno sobre el proceso de convergencia en materia de tecnología de la información y comunicación –TIC/ICPS el 27 de julio de 2015 y del Acuerdo de 21 de junio de 2016 relativo a dicho proceso de convergencia por el que se aprueba el documento ejecutivo “plan general de actuación en materia de convergencia TIC/ICPS”.

La actividad objeto de contratación, es necesaria para la prestación de los servicios, competencia de EJIE S.A., y está incluida en los servicios que pueden ser objeto de contratación (según Instrucción Sexta de la

Instrucciones sobre buenas prácticas en la contratación de servicios de Gobierno Vasco). Su prestación no puede ser asumida con los recursos humanos y técnicos de que dispone EJIE S.A., siendo además inviable su reorganización.

El presente pliego, como el resto de los documentos de la fase de preparación del contrato, incorporan las debidas garantías para dar cumplimiento a la Instrucción octava de las Instrucciones sobre buenas prácticas en la contratación de servicios de Gobierno Vasco.

1.2 Antecedentes

El contexto actual en materia de Ciberseguridad resulta cada vez más complejo. En un entorno en el que los procesos de digitalización están llegando a todos los ámbitos, la necesidad de conectividad y movilidad de todo tipo de dispositivos está en pleno auge.

Estas necesidades, en muchos casos, acaban haciéndose realidad en forma de múltiples dispositivos de todo tipo (IoT, OT, IoMT, etc.) conectados de forma no controlada a las redes LAN y WIFI, junto con los dispositivos IT (PCs, Portátiles, Impresoras, Equipos VoIP, etc.), sobre los que tradicionalmente sí suele existir un control y gestión más exhaustivo, y, potencialmente, con acceso a los Sistemas de Información IT (Servidores, BBDD, etc.) que son el objetivo principal de los Ciberataques en la actualidad.

Aunque en los últimos tiempos la situación va mejorando, en líneas generales, las empresas dedicadas a la producción de este tipo de dispositivos (IoT, OT, IoMT, etc.) no tienen la Seguridad entre sus prioridades y, en consecuencia, estos equipos suelen estar afectados por Vulnerabilidades de Seguridad. Las redes criminales, por su parte, son conscientes de esta situación y, de manera creciente y cada vez más dirigida, tratan de explotar estas vulnerabilidades para atacar los Sistemas de Información IT.

Las entidades a las que EJIE ofrece sus Servicios de Seguridad no son una excepción y, en concreto, el Sector Sanitario constituye uno de los ámbitos en los que más está creciendo el número de dispositivos conectados a la red, especialmente los dispositivos IoMT (Internet of Medical Things), con objeto de optimizar el trabajo realizado por los profesionales de la Salud y así, en última instancia, mejorar el servicio ofrecido a los pacientes.

Consciente de esta y otras situaciones, EJIE se encuentra en una fase continua de Evolución de los Servicios de Seguridad que ofrece, de cara a mejorar las capacidades ya disponibles y a la incorporación de nuevas capacidades y funcionalidades que permitan hacerles frente. Como punto de partida de esta fase de evolución, se realizó en el año 2020 un Plan Director de Seguridad que pretendía marcar el camino que debía seguir EJIE en materia de Ciberseguridad en los siguientes 4 años.

En línea con lo anterior, entre las iniciativas recogidas dentro del Plan Director de Seguridad, se identifican varias necesidades encaminadas a mejorar la Seguridad y Gestión de todo tipo de dispositivos conectados a la red, entre las que destacan, visibilidad e identificación de los dispositivos, control de acceso a la red, segmentación, control de comunicaciones, inventariado y gestión de vulnerabilidades.

En ausencia de elementos de seguridad que permitan llevar a cabo una segmentación de red y un control de acceso y comunicaciones entres segmentos, **se hace necesaria la contratación de servicios especializados de seguridad, que contemplen la provisión y puesta en marcha de una Infraestructura de Seguridad en Centros de Osakidetza**, de acuerdo al alcance y requerimientos técnicos y de servicio solicitados en la presente contratación.

El proyecto contempla como **alcance varios de los Centros de OSAKIDETZA**.

2 Objeto y Alcance del contrato

2.1 Objeto de la Contratación

El objeto del presente Pliego de Condiciones Técnicas es la contratación de servicios especializados de seguridad, que contemplen la provisión y puesta en marcha de una Infraestructura de Seguridad en Centros de Osakidetza, de acuerdo al alcance y requerimientos técnicos y de servicio solicitados en la presente contratación. Ello permitirá ofrecer unos Servicios de Seguridad, centrados en la segmentación y el control de acceso y comunicaciones entre segmentos, que hasta ahora EJIE no podía ofrecer con las herramientas disponibles en los Centros dentro del alcance.

Todo lo indicado en este apartado se engloba dentro del Plan de Recuperación, Transformación y Resiliencia - Financiado por la Unión Europea – NextGenerationEU

2.2 Alcance de la Contratación

El proyecto deberá considerar el siguiente alcance:

- Provisión y puesta en marcha de una Infraestructura de Seguridad en Centros de Osakidetza, incluyendo los trabajos de consultoría, diseño y configuración necesarios.
  La Infraestructura de Seguridad se centrará en la segmentación y el control de acceso y comunicaciones entre segmentos de los diferentes Centros de Osakidetza, estando basada en Firewalls en los propios Centros. También será parte del alcance la infraestructura centralizada de administración, logs y reporting para dichos Firewalls.
- La incorporación a esta nueva solución de los Centros de OSAKIDETZA que constituyen el alcance del proyecto, incluyendo todos los trabajos de consultoría, instalación y configuración necesarios para cada uno de los Centros.
- La dotación de productos (hardware y software) necesarios, junto con su soporte y garantía de fabricantes asociados.
- Servicios de seguimiento, gestión, transferencia de conocimiento y documentación del proyecto, incluyendo las tareas de modelado del servicio.
- Servicios de ajuste y acondicionamiento del servicio.
- Servicios de mantenimiento (Nivel 3) de la solución implantada.

En general quedan incluidos en el alcance del contrato el suministro e instalación y mantenimiento de todos los equipos necesarios para cubrir las necesidades planteada en el presente pliego con todos los medios

auxiliares necesarios, pequeño material, equipos de medida, herramientas, etc., así como todos aquellos elementos y operaciones que, aun no habiéndose citado específicamente, sean considerados necesarios para llevar a cabo las tareas requeridas para la ejecución del contrato.

Para todos los equipos incluidos en el presente pliego, se incluye el suministro, transporte, montaje en racks, conexionado, accesorios, así como la configuración y puesta en servicio, etiquetado, certificaciones y pruebas.

Todos los equipos, licencias y sus soportes asociados deberán ser oficiales y estar garantizadas por el fabricante.

Todos los equipos, software, licencias y documentación que componen la nueva solución de seguridad serán a su recepción propiedad de EJIE y deberán estar a su nombre.

Los elementos ofertados por el adjudicatario deben encontrarse en activo en el ciclo de vida de producto del fabricante, por lo que no se podrán ofertar elementos para los cuales ya haya prevista fecha de fin de ventas, garantizando que no se encuentre fuera de soporte al menos en los cinco (5) años siguientes a la fecha de presentación de la oferta.

Todos los suministros objeto del contrato se realizarán bajo una premisa de eficiencia energética orientada a la reducción de consumos energéticos.

2.3 Descripción de Situación

En este apartado se expone la situación actual en el ámbito de OSAKIDETZA, lo cual, en general, es aplicable a los Centros que serán alcance del proyecto. También se expondrá la evolución prevista a medio plazo en los aspectos que pueden influir en este proyecto. El contenido es el siguiente:

2.3.1 Seguridad Dispositivos

2.3.2 Roadmap Seguridad Dispositivos.

2.3.3 Información de Contexto

2.3.3.1 OSAKIDETZA

2.3.3.2 BATERA

*Esta información se considera **confidencial**, por lo cual los licitadores interesados en recibir estos datos deberán seguir las instrucciones indicadas en el **apartado 20.Confidencialidad del PCP** del presente expediente y procedimiento de la cláusula 67.4 del PCP.*

2.4 Modelo de Servicio

2.4.1 Alcance del Servicio

Como se ha comentado previamente, el objetivo de Osakidetza con este expediente es, dentro del Roadmap estratégico de Seguridad de Dispositivos, implementar en los Centros que forman parte del Proyecto ARO Digitala una Infraestructura de Seguridad basada en Firewalls, que permita segmentar la red de los Centros y realizar un control de las comunicaciones entre los diferentes segmentos, entre los que se encuentran los segmentos donde se ubicará el equipamiento IoMT para Imagen Digital.

En línea con el diseño global del Proyecto ARO Digitala y, por lo tanto, con las necesidades existentes de ancho de banda en los diferentes Centros que forma parte de este proyecto, se diferencian, como ya se ha comentado previamente, dos tipos de centro de cara a este proyecto:

- **Centros Tipo A**: Centros que forman parte del proyecto ARO Digitala que se prevé que dispongan de un ancho de banda en WAN de hasta 30 Gbps.
- **Centros Tipo B**: Centros que forman parte del proyecto ARO Digitala que se prevé que dispongan de un ancho de banda en WAN de hasta 5 Gbps.

Esta clasificación se realiza con objeto de determinar dos modelos diferentes de Firewall a implantar en función del tipo de centro.

A continuación se muestra una tabla donde se enumeran los **Centros de Osakidetza que constituyen el alcance de este proyecto**, indicando el Tipo de Centro al que corresponde cada uno de ellos:

CENTRO	TIPO CENTRO FW
AMBULATORIO AMARA BERRI	TIPO A
AMBULATORIO BUENA VISTA	TIPO A
AMBULATORIO DE DEUSTO	TIPO A
AMBULATORIO DE DR. AREILZA	TIPO A
AMBULATORIO LAS ARENAS	TIPO A
AMBULATORIO REPELEGA	TIPO A
AMBULATORIO ZABALLA	TIPO A
CENTRO SALUD GROS	TIPO A
HOSPITAL ALTO DEBA	TIPO A
HOSPITAL BASURTO	TIPO A
HOSPITAL COMARCAL BIDASOA	TIPO A

CENTRO	TIPO CENTRO FW
HOSPITAL DE CRUCES	TIPO A
HOSPITAL DE DONOSTIA	TIPO A
HOSPITAL DE GALDAKAO	TIPO A
HOSPITAL DE MENDARO	TIPO A
HOSPITAL DE SAN ELOY	TIPO A
HOSPITAL DE SANTIAGO	TIPO A
HOSPITAL DE TXAGORRITXU	TIPO A
HOSPITAL DE ZUMARRAGA	TIPO A
HOSPITAL GERNIKA	TIPO A
HOSPITAL URDULIZ	TIPO A
ONKOLOGIKOA	TIPO A
AMBULATORIO AMARA CENTRO	TIPO B
AMBULATORIO BASAURI - ARIZ	TIPO B
AMBULATORIO BEASAIN	TIPO B
AMBULATORIO BOMBERO ETXANIZ	TIPO B
AMBULATORIO IRUN CENTRO	TIPO B
AMBULATORIO MARKONZAGA	TIPO B
AMBULATORIO REKALDE	TIPO B
AMBULATORIO SANTURTZI	TIPO B
AMBULATORIO SANTUTXU-SOLOKOETXE	TIPO B
AMBULATORIO TOLOSA	TIPO B
AMBULATORIO ZARAUTZ	TIPO B
CENTRO SALUD ALANGO	TIPO B
CENTRO SALUD ALGORTA	TIPO B
CENTRO SALUD AMOREBIETA-ETXANO	TIPO B
CENTRO SALUD LAKUA-ARRIAGA	TIPO B
CENTRO SALUD LEIOA	TIPO B
CENTRO SALUD LOS CASTAÑOS	TIPO B
CENTRO SALUD ONDARRETA	TIPO B
CENTRO SALUD RONTEGI	TIPO B
CENTRO SALUD SALBURUA	TIPO B
CENTRO SALUD SAN MARTIN	TIPO B
CENTRO SALUD ZABALGANA	TIPO B
CENTRO SALUD ZUAZO	TIPO B
DIRECCIÓN GENERAL	TIPO B
H. EIBAR	TIPO B
H.P. BERMEO	TIPO B
H.P. ZALDIBAR	TIPO B

CENTRO	TIPO CENTRO FW
H.P. ZAMUDIO	TIPO B
HOSPITAL GORLIZ	TIPO B
HOSPITAL LEZA	TIPO B
HOSPITAL SANTA MARINA	TIPO B
SALUD MENTAL BIZKAIA	TIPO B

En cada uno de estos centros, en función del tipo de centro, el licitador deberá ofertar un **Cluster de Firewall** que iguale o supere los diferentes requisitos mínimos que se detallarán en el apartado 3.

Además del cluster de Firewall que se deberá instalar en cada centro, según su tipo, será parte del alcance del proyecto la implantación de una **infraestructura centralizada de administración, logs y reporting** para los Firewalls distribuidos en los diferentes centros. Esta infraestructura centralizada se instalará en los CPDs principales de EJIE en:

- CPD EJIE: Avenida del Mediterráneo 14, 01010 Vitoria
- CPD ERANDIO: Sede del Departamento de seguridad, Erandio (DR)

La infraestructura virtual de gestión centralizada sí estará en DR mediante los mecanismos que aporte BATERA para el equipamiento virtual. La infraestructura HW de logs y reporting, si aplica en la solución propuesta, no se requiere que esté en DR en Erandio, todos los elementos estarán en el CPD principal de EJIE.

Por lo tanto, y a modo de resumen, se determina que el **ALCANCE** técnico inicial del proyecto lo constituye:

- Un (1) **cluster de Firewall en cincuenta y cuatro (54) Centros** de Osakideza:
  - **Centros Tipo A**: **Veintidós (22)** centros tipo A.
  - **Centros Tipo B**: **Treinta y dos (32)** centros tipo B.
- Una (1) **infraestructura centralizada de administración, logs y reporting** para los cluster de Firewall indicados en el punto anterior.

Los requisitos técnicos y funcionales de toda esta Infraestructura de Seguridad se detallarán más adelante en el apartado 3.

2.4.2 Periodo de Prestación del Servicio

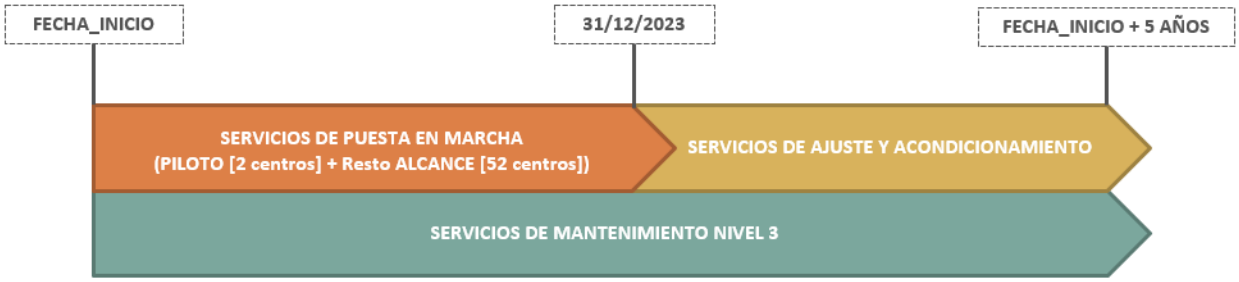
El contrato tiene un duración de 5 años desde la fecha del pedido.

Durante ese tiempo, se estima una fase de PILOTO inicial en la que se deplegará la solución en dos (2) centros, uno de cada Tipo A y B respectivamente. Esta fase tendrá una duración estimada de 2 meses (la duración depende en gran medida del periodo de suministro).

Superada la fase de PILOTO (2 centros), se desplegará la solución en todos los centros que forman parte del ALCANCE (52 centros adicionales) con una configuración mínima básica. Estas dos fases constituyen los Servicios de Puesta en Marcha y deben estar finalizados antes del 31/12/2023.

Superada esta fase, se pasa a una fase de Ajuste del Servicio que se puede extender durante toda la duración del contrato y, adicionalmente, durante todo el contrato, el licitador ofrecerá servicios de Mantenimiento (Nivel 3) del entorno.

Todo esto queda reflejado en el siguiente esquema:



El detalle de los requisitos técnicos y funcionales, así como de los servicios profesionales demandados se puede encontrar en próximos apartados en este pliego de condiciones técnicas.

3 Requisitos técnicos y funcionales

El licitador deberá tener en cuenta que el equipamiento y tecnologías a desplegar deben dar solución a los servicios de seguridad Firewall (FW) en los centros sanitarios, de acuerdo con los requerimientos definidos en el presente pliego.

A continuación, se enumeran los requerimientos del servicio, que deberán prestarse a través de la solución desplegada por el adjudicatario. Todos los requisitos solicitados se consideran obligatorios y deben estar licenciados en todos los equipos propuestos por los licitadores, salvo que se indique explícitamente que no lo son.

Como se indica posteriormente, como documentación anexa a la propuesta técnica, el licitador deberá adjuntar el **checklist de requerimientos** solicitado a través del presente expediente, que recoge la revisión de desempeño tanto de los requisitos de obligado cumplimiento como de algunas características que tienen requisitos mínimos a cumplir.

3.1 Requisitos Diseño de la Solución

Como se ha adelantado previamente, la solución debe plantear un diseño que cumpla, al menos, los siguientes requisitos obligatorios:

- La solución debe tener en consideración toda la información de contexto expuesta en los apartados 2.3 y 2.4 para su diseño, debiendo ser compatible con lo expuesto en dichos apartados.

  En esa línea, son relevantes de cara al diseño los siguientes aspectos, algunos ya mencionados en la información de contexto y otros más detallados en siguientes apartados:

  - Gestión: Será infraestructura centralizada y podrá, idealmente, ser virtual y albergada en BATERA (Tenant Osakidetza), proveiendo EJIE la infraestructura para albergar este equipamiento virtual
  - Logs y Reporting: Será infraestructura centralizada en los CPDs de BATERA y podrá, idealmente, ser virtual y albergada en BATERA (Tenant Osakidetza), proveiendo EJIE la infraestructura para albergar este equipamiento virtual.

    Para poder hacer uso de la infraestructura proporcionada por EJIE, la solución debería admitir el uso de almacenamiento vía NFS. No es viable ofrecer todo el almacenamiento que se requiere para esta solución (al menos 40TB) como almacenamiento principal asociado a una OVA o Máquina Virtual. Es decir, la solución debería consistir en, al menos, un servidor virtual de logs y reporting albergado en BATERA cuyo almacenamiento de logs se pueda mapear, como mínimo, vía NFS.

    En caso de no poder hacer uso de la infraestructura proporcionada por EJIE, el licitador deberá proveer la infraestructura HW y SW relacionada con el almacenamiento de logs centralizados, debiendo consistir en este caso la solución en appliances propios del fabricante con, al menos, este propósito específico, no siendo válidas soluciones genéricas de virtualización o almacenamiento.

  - Firewall Centros: Se tratará de clusters de Firewall HW que, al menos y en una primera fase, aislará las VLANs de los Centros que no sean de usuario y VoIP. Es decir, las redes de Usuario y VoIP, en principio, no quedarían segmentadas y protegidas por estos Firewall. Sí estarían protegidas las redes de servidores, IoT, OT e IoMT, etc. Esto hace que estos cluster de Firewall pasen a ser elementos críticos dentro de las redes de los Centros de Osakidetza.

- Módulos licenciados: Como mínimo estarán licenciados los módulos de Firewall, IPS, Identificación de Usuarios, Rutado Avanzado (Protocolos de rutado dinámicos, PBR), Gestión centralizada, Logs centralizados, Reporting centralizado. Los nombres de los módulos son genéricos, cada fabricante tendrá un nombre específico para el módulo equivalente.

- Gestión centralizada: La solución debe permitir una gestión centralizada en un único punto de todo el equipamiento.
- Logs y Reporting centralizado: La solución debe centralizar los logs de todos los Firewall que constituyen la solución. Asimismo, debe ser capaz de analizar esos logs y generar informes de manera centralizada y teniendo en cuenta los datos de todo el equipamiento de forma global o individual por centro.
- Solución de Gestión, Logs y Reporting robusta, flexible y escalable: Al tratarse de una solución centralizada de la que dependen para su gestión y reporting múltiples elementos, debe ser una solución robusta, flexible y escalable. Para ello:

    - ✓ Si la propuesta del licitador no puede albergarse completamente en BATERA y requiere hardware propio, estos elementos hardware relacionados con gestión, logs o reporting deben estar duplicados y sus datos sincronizados, de forma que la pérdida de uno de los elementos no suponga una pérdida de datos. Cada elemento hardware deberá llevar doble fuente de alimentación.
    - ✓ La solución debe permitir la incorporación a la gestión, logs y reporting de nuevos equipos Firewall de forma flexible, tanto en cantidad como en tipología (mismos modelos ofertados u otros diferentes), a lo largo de la vida del contrato.

  Como se ha comentado previamente, la infraestructura virtual de gestión y logs centralizada proporcionada por BATERA sí podrá estar en DR mediante los mecanismos que aporte BATERA para el equipamiento virtual. La infraestructura HW de logs y reporting suministrada por el licitador, si aplica en la solución propuesta, no se requiere que esté en DR en Erandio, todos los elementos estarán en el CPD principal de EJIE.
- Todos los elementos alcance de este contrato tendrán dedicación exclusiva a este proyecto, no pudiendo reutilizarse ninguna plataforma existente actualmente en el ámbito de EJIE/BATERA/OSAKIDETZA.
- El elemento Firewall de los centros realizará, al menos, funciones de networking, segmentación, seguridad y control de acceso.
- Los elementos Firewall de los centros deben constituir una solución robusta, flexible y escalable: Los cluster de Firewall van a constituir elementos críticos dentro de la red de cada centro y, como tales, deben constituir una solución:

    - Robusta: Deberán constituir un cluster en HA (Activo/Pasivo) o Balanceo de Carga (Activo/Activo), debiendo poder asumir todo el tráfico en caso de caída de uno de los equipos que constituyen el cluster. Cada equipo deberá llevar doble fuente de alimentación.

      En caso de optar por soluciones activo-activo, no se permite la utilización de tráfico multicast a ningún nivel (nivel 2 o nivel 3) para la implementación del cluster en las redes de servicio y gestión. Podría utilizarse en redes de heartbeat, aunque no es deseable. El licitador deberá explicar en detalle el modo en que funciona el modo de cluster propuesto en su diseño.

      El licitador deberá tener en cuenta que, en algunos centros, cada nodo puede tener que ir ubicado en una localización diferente dentro del centro (separados por decenas/cientos de metros), existiendo en todo caso una extensión a nivel 2 entre ambas ubicaciones.

    - Escalable: Existe incertidumbre en relación a la cantidad de tráfico que deberán procesar estos equipos a medio/largo plazo. Está previsto que protejan las redes de Imagen Digital. Esas redes,

actualmente consumen un tráfico sin determinar entre los equipos de Imagen y los servidores centrales. Esos requisitos está previsto que crezcan en dos sentidos:

- Nº Equipos de Imagen: Está previsto el crecimiento del número de equipos de imagen. Es decir, aumentará significativamente el tráfico entre el segmento de red de Imagen y el/los servidores de imagen. Misma red de origen (directamente conectada a Firewall), Misma IP destino (en CPD Central alcanzable a través de interfaz externo firewall), Mismos puertos, más tráfico.
- Calidad Imagen: Está previsto el crecimiento en la calidad de las imágenes enviadas, pasando de 2D a 3D y a mayores resoluciones. Es decir, aumentará significativamente el tráfico entre los mismos equipos existentes de Imagen y los servidores centrales: Misma IP origen (en red directamente conectada a Firewall), Misma IP destino (en CPD Central alcanzable a través de interfaz externo firewall), Mismos puertos, más tráfico.

Estos datos se proporcionan con objeto de que el licitador tenga claro cómo debería repartir la carga el cluster de Firewall que proponga. No se trata de un crecimiento típico y, por ese motivo, se quiere detallar este aspecto.

Debido a la incertidumbre, se va a determinar un throughput mínimo que deberán procesar los Firewall en función del tipo de centro. Así, la solución propuesta por el licitador deberá, al menos, igualar o superar ese throughput según el tipo de centro.

Aunque se considera que los throughtput solicitados serán suficientes a largo plazo, idealmente, aunque no de forma obligatoria, la solución de cluster de Firewall propuesta debería ser escalable, aportando valor:

- Que el crecimiento del cluster pueda realizarse sin corte de servicio
- Que el escalado en throughput sea lineal (crecimiento en throughput de al menos un 80% de la capacidad de los nodos incorporados)
- Que el crecimiento no requiera cambios de diseño de red para hacer uso de los nuevos nodos.

El licitador deberá explicar en detalle el modo en que escala el cluster propuesto en su diseño en caso de permitir escalar.

- Flexible: La solución en los centros deberá tener margen para adaptarse a configuraciones futuras en lo que a segmentación y políticas de seguridad se refiere.

3.2 Requisitos Firewalls Centros

3.2.1 Modelos y Cantidad

Como ya se ha adelantado previamente, se determina la existencia de dos tipos de centros en Osakidetza de cara a este proyecto:

- **Centros Tipo A**: Centros que forman parte del proyecto ARO Digitala que se prevé que dispongan de un ancho de banda en WAN de hasta 30 Gbps.

- **Centros Tipo B**: Centros que forman parte del proyecto ARO Digitala que se prevé que dispongan de un ancho de banda en WAN de hasta 5 Gbps.

El licitador deberá presentar dos modelos de solución de Firewall para adaptarse a estos dos tipos de centros diferentes. En cada caso, deberá presentar un Cluster de, al menos, e idealmente, dos nodos iguales. El licitador deberá tener en cuenta que, en algunos centros, cada nodo puede tener que ir ubicado en una localización diferente dentro del centro, existiendo en todo caso una extensión a nivel 2 entre ambas ubicaciones.

A continuación se indican los tipos de Firewall y las cantidades mínimas requeridas (se indica mínimas por si algún licitador propone clusters de más de dos nodos):

Modelo Firewall	Cantidad Mínima de Equipos
Modelo Centro Tipo A	2 x 22
Modelo Centro Tipo B	2 x 32

3.2.2 Hardware

A continuación, se muestra una tabla con los requisitos mínimos que debe cumplir la solución propuesta por el licitador para cada tipo de centro. El incumplimiento de estos requisitos supondrá la exclusión del licitador:

Requisito mínimo	Por Firewall / Por Cluster	Modelo Centro Tipo A	Modelo Centro Tipo B
Rendimiento mínimo con los módulos FW e IPS activados (*2)	Por Cluster	>= 10 Gbps	>= 3,75 Gbps
Rendimiento mínimo con el modulo FW activado	Por Cluster	>= 20 Gbps	>= 5 Gbps
Rendimiento máximo con los módulos FW e IPS activados (*2)	Por Firewall	20 Gbps	7,5 Gbps
Interfaces 1GE RJ45 (*1)	Por Firewall	4	4
Interfaces 10GE SFP+ SR MM LC (*1)	Por Firewall	-	2
Interfaces 40GE QSFP+ SR4 MM MPO (*1)	Por Firewall	2	-
Fuentes de alimentación redundantes (*3)	Por Firewall	SÍ	SÍ

(*1) Los Firewall deberán ser suministrados, al menos, con los interfaces mínimos indicados en la tabla. El licitador también deberá suministrar los latiguillos de conexión hasta el switch, ubicado en el mismo armario.

(*2) Los datos deben corresponder a **medidas realizadas con tráfico real/empresarial y con, al menos, los módulos de FW e IPS activados,** no siendo válidas las medidas en condiciones ideales. Este dato se debe proporcionar respaldado por información proporcionada por el fabricante, quedando excluidas las soluciones que no presenten estas medidas claramente respaldadas.

(*3) Los Firewall deberán ser suministrados con fuente de alimentación redundante.

Para dar respuesta a estos requisitos por ejemplo, para el Centro Tipo A, un licitador podría optar por presentar diferentes opciones, debiéndose decantar por una de ellas únicamente en la oferta. A continuación se muestran a modo de ejemplo dos de las posibles opciones, pudiendo existir otras alternativas que cumplan requisitos:

- Idealmente, un Cluster de 2 nodos (activo/pasivo o activo/activo) en el que cada nodo proporcione, al menos, 10Gbps IPS y 20 Gbps FW.

- Un cluster de 3 nodos (activo/activo/activo) en el que cada nodo proporcione 5 Gbps IPS y 10 Gbps FW (suponiendo que escalen linearmente, que no tiene por qué ser así). Recordar que ante el fallo de un nodo, el resto debe poder asumir todo el tráfico y cumplir los mínimos solicitados.

El licitador deberá ajustar el equipamiento propuesto a las soluciones ideales requeridas. Proponer equipos más pequeños que con clusters de 3 o más equipos lleguen al mínimo requerido no supondrá una ventaja económica puesto que, a nivel económico, se valorará el precio/Gbps de la solución completa cuando trabaja con un único nodo. Esto quedará reflejado en el anexo económico y los criterios de valoración que se determinarán en el PCP, donde se tendrán en cuenta los datos que el licitador debe presentar en la siguiente fila de la tabla del CheckList y en la propia oferta técnica:

Requisito	Por Firewall / Por Cluster	Modelo Centro Tipo A	Modelo Centro Tipo B
Rendimiento del equipo propuesto con los módulos FW e IPS activados en Gbps. (*1) (*2) (*3)	Por Firewall	_____ Gbps	____ Gbps

(*1) Los datos deben corresponder a **medidas realizadas con tráfico real/empresarial y con, al menos, los módulos de FW e IPS activados,** no siendo válidas las medidas en condiciones ideales. Este dato se debe proporcionar respaldado por información proporcionada por el fabricante, quedando excluidas las soluciones que no presenten estas medidas.

(*2) Se admite hasta 1 decimal en la medida. Por ejemplo, 10,1 Gbps.

(*3) Esta medida se utilizará en el modelo económico del PCP para ponderar el precio/Gbps de la solución.

Por otra parte, proponer equipos sobredimensionados para mejorar ese precio/Gbps tampoco es viable, ya que se ha añadido en la tabla un requisito en el que se marca el máximo alcanzable por cada equipo, según el tipo de centro.

3.2.3 Funcionalidades

Todos los firewall propuestos para los diferentes tipo de centro deben cumplir de forma individual, al menos, los siguientes requisitos obligatorios, que deben estar licenciados:

Networking:

- Gestión fuera de banda: Puerto de gestión dedicado y puerto de consola.
- Dual Stack: IPv4 e IPv6
- VLANs: Deberá soportar 802.1Q

- LACP: Deberá soportar LACP 802.3ad para poder agregar interfaces.
- VoIP: Debe soportar tráfico VoIP, como mínimo, sobre los protocolos SIP, H.323, RTP, SCCP. Debe soportar NAT para estos protocolos.
- NAT: Deberá soportar NAT IPv4 en todas sus variantes 1:1, N:1, Port forwarding.
- Routing: Los equipos deberán soportar:

  - ✓ Rutado estático tradicional
  - ✓ Rutado basado en política (PBR)
  - ✓ Protocolos de rutado dinámico: RIP v1 y v2, OSPF, BGP, Multicast
- DHCP: Deberá ser capaz de actuar como servidor DHCP en todos sus interfaces de red. También debe soportar DHCP Relay.
- Gestión de ancho de banda y priorización del tráfico. Las soluciones deben proporcionar funcionalidades de control de ancho de banda en base a parámetro de red y aplicación, y posibilitar reservas de ancho de banda para determinado tipo de tráfico, establecer límites y priorizar un tráfico frente a otro.

Seguridad, autenticación y delegación:

- FW: Debe permitir crear políticas flexibles y granulares, teniendo en cuenta IPs, usuarios, puertos, aplicaciones y protocolos. Permitirá crear reglas con horarios. Permitirá decidir el nivel de Log de cada regla individualmente
- Objetos: Deberá permitir definir objetos de diferentes tipos para utilizar en las políticas. Como mínimo, deberá permitir definir objetos por IP, red, rangos de IPs, geolocalización, FQDN y objetos dinámicos que representen aplicaciones en nube (Aplicaciones Cloud ámbito Microsoft como mínimo).
- Protocolos dinámicos: Debe interpretar y abrir dinámicamente reglas para los protocolos dinámicos más comunes: DCE/RPC, FTP, H.245 I, H.245 O, H.323, MGCP, MMS, PMAP, PPTP, SIP, TNS (Oracle), TFTP
- IPS: El equipamiento deberá ofrecer la funcionalidad de IPS, con actualización de firmas automática. El IPS deberá estar basado tanto en firmas, como en anomalías de protocolos y detecciones basadas en conducta. Se deberán poder consultar capturas de tráfico para los eventos de IPS.
- Control de Usuarios: Capacidad de identificación de usuarios, con integración con Directorio Activo de Microsoft. Se podrán crear reglas en base a usuarios y grupos de Directorio Activo.
- Capturas de tráfico: Debe permitir capturar tráfico para monitorización en tiempo real, así como a ficheros en formato PCAP.
- NetFlow: La solución debe soportar NetFlow o equivalente (sflow, etc.) para monitorización de tráfico de red.
- Monitorización: Debe soportar monitorización del equipamiento vía SNMP v1, 2 y 3
- Syslog: Debe soportar reenvío de logs vía syslog.

Otros Requisitos:

- Certificaciones de Seguridad: Como mínimo deberá cumplir la siguiente certificación de seguridad:

  - ✓ CCN-CERT: Ante la existencia de servicios del ámbito de la Sanidad de categoría ALTA en el ámbito del Esquema Nacional de Seguridad, EJIE tiene la obligación de adecuar sus sistemas de

información a las medidas establecidas en dicho nivel, por lo que se deberá cumplir que los productos presentados por el licitador estén recogidos en el catálogo de productos certificados del CCN (Guía de Seguridad de las TIC CCN-STIC 105) o, como medidas alternativas, que se pueda evidenciar que están en proceso o que lo estén versiones/modelos inferiores o anteriores del producto (versiones publicadas hace menos de 2 años).

3.3 Requisitos Gestión, Logs y Reporting centralizado

Como ya se ha comentado previamente, se requiere una infraestructura que permita centralizar la gestión, almacenamiento de logs y reporting de toda la Infraestructura de Seguridad alcance de este proyecto.

Además de los requisitos en este ámbito ya establecidos en el apartado de Requisitos de Diseño de la Solución, la solución deberá cumplir, al menos, los siguientes requisitos obligatorios:

- Aunque todos los equipos de los centros estarán gestionados y reportando logs de manera centralizada, un fallo de comunicación bien con la gestión o bien con el servidor de logs no debe impactar en su funcionamiento.
- La solución debe permitir desplegar políticas de forma centralizada en todos los Firewall de los centros, dando la opción de que parte de la política sea común a todos los equipos y parte de la política sea específica de algunos equipos. De esta forma, un cambio en la zona común aplicaría a todos los equipos y un cambio en la zona personalizada únicamente aplicará a los equipos especificados.
- Almacenamiento y consolidación centralizada de logs de registro/seguridad y obtención de informes (reporting) de uso del servicio. Se dispondrá de un repositorio centralizado donde almacenar todos los logs generados por la infraestructura de seguridad con una capacidad mínima de 40TB. Como se ha comentado previamente, en caso de optar por solución HW propia, este entorno debe ser tolerante a fallos hardware, de forma que, ante el fallo irreversible de un equipo completo, otro siga dando el servicio sin pérdida de funcionalidad ni de datos.

  Al ser un entorno nuevo no se dispone de un dimensionamiento en cuanto a logs/segundo que puede requerir el entorno. Se solicita que, al menos, la solución sea capaz de recibir 300 GB/día.

- En caso de optar por una solución de gestión y logs en cloud pública, la solución deberá albergarse en un DataCenter en la Unión Europea para asegurar el cumplimiento de la legislación vigente.
- Usuarios administradores: Como mínimo, deben poder ser locales, integrados con Directorio Activo de Microsoft, con RADIUS y con TACACS+.
- Roles de administración: Deberá permitir diferentes roles de administración (lectura, escritura). Debe admitir roles que permitan delegar el acceso en modo lectura a parte de la administración y el acceso en modo escritura a otros módulos. Asimismo, debe permitir la creación de roles que permitan la gestión en lectura/escritura de sólo una parte de la infraestructura.
- Monitorización centralizada: El sistema debe posibilitar la visión en tiempo real del conjunto de la solución, estado de los equipos y tráfico gestionado. La actividad podrá consultarse en tiempo real a nivel de centro individual y de forma agregada (conjunto de la red).
- La solución debe permitir la integración de sus logs y de sus alertas con herramientas de SIEM. En concreto, debe permitir la integración con el SIEM de EJIE basado en SPLUNK CLOUD.
- La solución debe registrar los cambios realizados en las políticas definidas. Asimismo, debe ofrecer la posibilidad de comparación con políticas previas y de recuperación de las políticas previas en caso de fallo. Las interfaces gráficas para trabajar a la hora de definir y desplegar políticas particulares deben ser sencillas e intuitivas.

- La solución debe incorporar mecanismos de verificación y validación de las políticas antes de su implementación y mecanismos para regresar a las políticas previas en caso de fallo.
- Automatización: La solución debe permitir la automatización de la configuración de políticas, como mínimo, vía REST API.
- Los informes de servicio que proporcionen las plataformas deben contemplar al menos información de estadísticas de uso de servicio y consumo de ancho de banda, amenazas de seguridad, aplicación de políticas y control de aplicaciones. Estas estadísticas e informes podrán consultarse y generarse tanto por centro individual como también en su totalidad agregada.
- La solución debe permitir programar informes mensuales globales o diferenciados por centros.
- Centralización de backups y configuraciones: La solución debe permitir mantener, de forma centralizada, backups y configuraciones de todo el equipamiento que constituye la infraestructura.

3.4 Checklist de requerimientos

Como documentación anexa a la propuesta técnica, el licitador deberá adjuntar el checklist de requerimientos solicitado a través del presente expediente. La oferta no se debe limitar a responder a este checklist. Este documento es una ayuda a la evaluación. Hay requisitos que se especifican en el presente pliego de condiciones técnicas que no aparecen en el checklist por no ser "ítems" o "checks" claramente identificables, pero que deben ser detallados en la oferta. Ver anexo 5.1 "**Anexo I PCT – Checklist Requisitos Técnicos**"

4 Servicios Profesionales

Los servicios profesionales se dividen en tres partes diferenciadas:

- **Servicios de Puesta en Marcha:**
  Se trata de los servicios de aprovisionamiento y puesta en marcha inicial de la Infraestructura de Seguridad. En los centros únicamente se hará una instalación básica inicial.

- **Servicios de Ajuste y Acondicionamiento:**
  Se trata de servicios previstos para, en respuesta a la estrategia de Osakidetza en materia de seguridad corporativa y en coordinación con otros proyectos relacionados con el control de acceso a la red de dispositivos IT, IoT, IoMT, ajustar segmentación y configuraciones en los FW de los centros, aplicando una combinación de configuraciones comunes de toda la organización y específicas de cada centro.

- **Servicios de Mantenimiento Nivel 3**
  Se trata de los servicios de mantenimiento típicos de Nivel 3 que se detallan más adelante.

A continuación se muestra un esquema de estos servicios donde se ve la escala temporal de los mismos:



4.1 Servicios de Puesta en Marcha

La empresa adjudicataria deberá considerar, entre los servicios a prestar, el proyecto para el aprovisionamiento y puesta en marcha de la Infraestructura de Seguridad en los Centros de Osakidetza objeto de este pliego.

Para el aprovisionamiento y la puesta en marcha de la solución, se identifican al menos los siguientes trabajos a realizar por la empresa adjudicataria:

- Servicios de consultoría y diseño de la solución.
- Plan de actuación en los centros sanitarios.
- Servicios de instalación, configuración y puesta en marcha.
- Otros servicios de definición previos al despliegue.
- Documentación.
- Transferencia de conocimiento.

El adjudicatario deberá tener en cuenta que la implantación puede implicar diferentes diseños y plan de actuación e implantación adaptados al escenario previamente identificado en la fase de consultoría de los distintos Centros objeto de este pliego. Así, el servicio y la plataforma quedará operativa una vez concluido el alcance inicial, documentación y la transferencia de conocimiento.

4.1.1 Servicios de consultoría y diseño de la solución

Al inicio del contrato el adjudicatario deberá revisar conjuntamente con EJIE:

- Las características de la propuesta técnica del adjudicatario.
- Las características de la situación actual de los Centros: Arquitectura y configuración de red, aspectos relacionados con instalación física (ubicación, fuerza, cableado,…), etc.
- La relación de datos de partida disponibles sobre el equipamiento.
- Los requisitos preliminares y características mínimas solicitadas sobre la nueva solución: características firewalls, gestión centralizada, logs, reporting, etc.

Conocida la situación de partida y objetivos preliminares para la instalación de la solución, el adjudicatario deberá realizar servicios de consultoría e ingeniería para el diseño de la misma, incluyendo entre otros aspectos:

- Definición de la arquitectura física y lógica del sistema de seguridad junto a su correspondiente descripción detallada.
- Revisión/adecuación de criterios y requisitos de cobertura, seguridad, control de acceso, segmentación, gestión centralizada, rendimiento, etc. a considerar para el despliegue de las soluciones en centros.
- Políticas de configuración de los equipos que componen la solución.

El diseño y los diferentes criterios establecidos para el despliegue de la solución se validarán conjuntamente con EJIE.

4.1.2 Plan de actuación en los centros sanitarios.

El adjudicatario deberá elaborar un plan de actuación para garantizar la continuidad del servicio indicando todas las tareas previstas, garantizando que el impacto a los centros sanitarios sea el mínimo posible:

- El objetivo es garantizar la continuidad del servicio, y que los usuarios no perciban afección al servicio (o esta sea mínima).

- Se deberá plantear si procede, planes de actuaciones diferenciados atendiendo a diferentes casuísticas que se puedan encontrar en cada hospital.
- El adjudicatario deberá realizar los replanteos necesarios en los centros sanitarios con el objetivo de verificar todos los aspectos necesarios para una correcta instalación y puesta en marcha de los equipos. La información recolectada en estos replanteos deberá quedar reflejada en los planes de actuación.
- El plan deberá identificar las diferentes fases en las que acometer la instalación, conociendo la situación actual y prevista y establecer e identificar las limitaciones, impactos en los plazos, así como las diferentes necesidades de acuerdo a la estrategia de instalación en todos los centros objetos al alcance.
- Por otro lado, dependiendo de la situación actual y modelo de centro podrán considerarse planes y estrategias diferentes.
- Se realizará una instalación inicial básica que comprende la instalación y configuración inicial del cluster de Firewall de cada centro. Entre los trabajos básicos, se incluye, al menos, la conexión y configuración de los puertos de gestión, conexión y configuración de interfaces de servicio, reglas básicas, y dejar el equipo conectado a la gestión, logs y reporting centralizados. La instalación y puesta en marcha de ésta instalación básica de los equipos de todos los centros se deberá abordar **antes del 31/12/2023**, debiendo existir un compromiso del licitador y del fabricante propuesto en relación a los plazos de suministro de equipamiento y ejecución de los servicios de puesta en marcha.
- EJIE seleccionará ciertos centros sanitarios piloto (2 centros: 1 Tipo A y 1 Tipo B) cuya instalación deberá efectuarse antes de de comenzar el despliegue masivo. La instalación de estos centros se llevará a cabo tan pronto sea posible a partir de la fecha de firma del contrato (previamente deberán estar operativas las plataformas de gestión, logs y reporting)
- Respecto a la instalación de las plataformas de gestión, logs y reporting, deberá efectuarse de tal forma que estén operativas antes de la instalación del primer equipo (el primer equipo será el correspondiente a uno de los centros seleccionados como piloto).
- El adjudicatario deberá tener en cuenta que las actuaciones en los centros sanitarios para minimizar el impacto de las mismas: **podrán ser en cualquier momento**, en principio se van a ejecutar fuera de horario laboral pudiéndose realizarse los sábados, domingos y/o festivos o en horario nocturno (22h-8h)., en consecuencia el calendario para la ejecución y prestación de servicios profesionales en centros se debe poder ajustar a la actividad de de cada centro sanitario y en coordinación con EJIE/Osakidetza, solicitandose la ejecución de trabajos fuera de horario laboral sin coste adicional y asumiendo la replanificación de visitas que fuera necesario realizar a petición de Osakidetza.

4.1.3 Servicios de instalación, configuración y puesta en marcha

El adjudicatario deberá considerar la prestación de todos aquellos servicios que sean necesarios para la puesta en marcha de la solución, como son:

- Traslado e Instalación de equipamiento necesario en centros, así como equipamiento central, si aplica, en CPDs EJIE y Erandio, junto a la conectividad requerida para configuración de la arquitectura propuesta, en coherencia con la arquitectura de solución propuesta y validada previamente por EJIE.
- El adjudicatario deberá considerar las directrices que se establezcan en los centros en lo relativo a la adecuada instalación de equipos en centros y su identificación.
- El adjudicatario deberá tener en cuenta y respetar los estándares de parcheo en los armarios de los centros sanitarios.
- La definición de plantillas de configuración para dejar los equipos en gestión, configuración de las interfaces correspondientes y de las reglas básicas de los equipos para la puesta en marcha de las soluciones y servicios a instalar, incluyendo las plataformas de administración y reporting, así como la elaboración de plantillas para aplicación de políticas previamente acordadas entre el adjudicatario y EJIE.
- Elaboración del conjunto de planes de pruebas y su ejecución necesarios para confirmar que las soluciones quedan convenientemente operativas, las diferentes funcionalidades probadas e implementadas, de acuerdo a los requerimientos establecidos en el presente pliego.
- Establecimiento de unos primeros centros sanitarios (2 centros: 1 Tipo A y 1 Tipo B) como centros piloto antes de proceder con el despliegue masivo, para la cual el adjudicatario podrá emplear alguno de los equipos alcance de suministro. Las pruebas piloto tienen como objetivo:

    - ✓ Validar la solución técnica. Resolver dudas técnicas que puedan surgir con la activación del servicio.
    - ✓ Confirmar in situ el alcance y trabajos a realizar en cada centro. Resolver dudas con relación a dicho alcance y medir esfuerzos.
    - ✓ Validar la estrategia de actuación (Plan de actuación) para garantizar la continuidad del servicio.
    - ✓ Confirmar resto de procedimientos de ejecución y metodologías acordadas en inicio y adecuarlos, si se procede con algún cambio.
    - ✓ Confirmar los parámetros de configuración de los diferentes equipos.
    - ✓ Validar la relación de entregables esperados. Modificar las plantillas de documentos en caso necesario.

Una vez realizadas las pruebas y analizados los diferentes resultados, el adjudicatario deberá, en caso de necesidad:

- Adecuar el Plan de Actuación a adoptar en los centros, concretando las diferentes necesidades y servicios a considerar en el despliegue, esfuerzos requeridos, y recursos a disponer.
- Revisar y adecuar otros procedimientos y metodologías de ejecución, control y seguimiento; adecuación de plantillas de documentación etc.
- Adecuar aspectos técnicos sobre el diseño de la solución y su parametrización, para garantizar el cumplimiento de los criterios definidos en el presente pliego.
- Adecuar el Plan global del proyecto a partir de los puntos anteriores.

  El plan global de proyecto que se presente en oferta y posteriormente con el inicio del contrato, deberá reflejar la ejecución de estos centros piloto, considerando esta una **fase a superar antes del inicio de cualquier trabajo en el resto de centros**.

  Las propuestas de centros piloto (2 centros: 1 Tipo A y 1 Tipo B) se definirán conjuntamente con EJIE.

- Elaboración de la documentación relativa a las soluciones finalmente desplegadas.

4.1.4 Otros servicios de definición previos al despliegue

Como parte de los trabajos a realizar previos al despliegue, el adjudicatario deberá:

- Elaborar una Planificación global de Proyecto (y sus revisiones), teniendo en cuenta el diseño establecido y los planes de actuación acordados, con indicación de medios necesarios para su cumplimiento e hitos principales.
- Elaboración de un Análisis de riesgos, considerando el global del proyecto, y propuestas para mitigación de los mismos.
- Elaboración conjunta de procedimientos y metodologías de trabajo que sean necesarias para garantizar la correcta ejecución de los trabajos en los centros sanitarios.
- Elaboración conjunta de procedimientos y metodologías orientados al seguimiento y control de avance del despliegue, y control documental.
- Definición y creación de las plantillas para el conjunto de documentación del proyecto, a elaborar en conjunto con EJIE, en el arranque del proyecto. Aplicando un diseño que permita aplicar las mismas plantillas en todos los centros.

Los resultados de estos trabajos previos se podrán revisar/actualizar según necesidad con EJIE durante el proyecto.

4.1.5 Documentación

El adjudicatario deberá documentar la solución desplegada y servicio configurado, completando la documentación necesaria para el modelado de lo que constituye un nuevo “Application Service” dentro del “Business Service” de Firewall (FW) ya existente, incluyendo, al menos:

- **Descripción y Diseño de la Solución:** Se describirá la arquitectura y configuración general de la solución desplegada, incluyendo:
  - Análisis técnico realizado.
  - Gestión del Servicio.
  - Tipologías: Características Principales y Beneficios.
  - Catálogo de reglas aplicadas.
  - Características de la plataforma.
  - Políticas de telemetría, políticas de remediación y acciones de respuesta acordadas, en caso de que aplique.
  - Configuración de las consolas y cuadros de mando, indicadores, alertas configuradas, informes automáticos definidos...

- **Inventario de Elementos y Documentación As-built por cada Centro Sanitario:** Al finalizar toda la instalación de cada centro sanitario y en un plazo máximo de un (1) mes, el adjudicatario deberá entregar toda la documentación asociada a la solución implementada, incluyendo como mínimo:
  - Proyecto técnico descriptivo del sistema, especificando arquitectura y conexiones entre los equipos.
  - Descripción de los equipos, especificando dimensiones, peso, características mecánicas, montaje, instalación y conexión.
  - Manual de funcionamiento que describa con detalle el cometido y funcionamiento eléctrico y electrónico de los elementos instalados.
  - Manuales de mantenimiento.
  - Documento con la descripción de los Procedimientos vinculados a la Gestión del Soporte de fabricante y Garantías (gestión RMA) del equipamiento suministrado para el periodo en cuestión, teniendo en cuenta los niveles de servicio solicitados en cada caso.
  - Manual de explotación, detallando los procedimientos a seguir para la realización de los pertinentes ajustes, revisiones y mantenimiento de los equipos. Se incluirán normas precisas de mantenimiento, interpretación de errores más frecuentes y método de resolución, relación

de averías más probables y normas para su reparación (ajuste, preventivo y correctivo) y resúmenes de comandos.

- Inventario de equipo, incluyendo fabricante, modelo, número de serie, fecha de instalación, etc.
- Descripción detallada de las aplicaciones software y licencias (número de serie, clave de activación, nombre del usuario, número de usuarios autorizados, código de autorización, etc.).
- Archivos de configuración de equipos.
- Documentación que se genere vinculada a la transferencia de conocimiento.
- Actas de retirada y entrega de material, según sea el caso.
- Protocolos de pruebas.

- **Documentación para entrega del servicio a Operación, el cual da respuesta a los siguientes conceptos:**
  - Gestión del Conocimiento: Descripción y características generales del entorno, descripción de los distintos elementos que conforman la plataforma con el rol que desempeñan, configuraciones especificas a tener en cuenta, diseño y arquitectura con los diagramas de red o topológicos de la solución incluyendo todos los elementos involucrados en la solución, así como los flujos de comunicaciones necesarios para su funcionamiento.
  - Gestión de Activos: Inventario detallado de activos.
  - Gestión de la Configuración: Detalle de las configuraciones siguiendo las mejores prácticas de fabricante y los estándares de EJIE.
  - Gestión de Backup: Definición de los backups configurados.
  - Gestión de Eventos: Definición de la monitorización necesaria y configurada en los entornos de EJIE, marcándose además la línea base que permita realizar un mantenimiento preventivo efectivo. También se definirán los logs y reporting configurados.
  - Catálogo de Peticiones: Identificación de las peticiones “tipo” que aplican a este entorno de cara a definirlas en las herramientas de ticketing.
  - Gestión de Incidencias: Identificación de las incidencias más relevantes que pueden darse en el entorno, así como la línea de actuación en cada caso.
  - Gestión de la Disponibilidad: Plan de pruebas realizados con resultados obtenidos.
  - Gestión del servicio y reporting.
  - Gestión del Cambio: Identificar los procesos y requisitos involucrados

- Gestión de Despliegues/Onboarding: Se identificarán los aspectos necesarios para la incorporación de una nueva entidad al Servicio, en caso de que aplique.
- Gestión de la Continuidad: Analizar e identificar los riegos sobre la continuidad del servicio para elaborar el plan de continuidad para aplicar las acciones necesarias para mantener la continuidad del servicio.
- Gestión de la Capacidad: Se identificarán los elementos a controlar para mantener la capacidad del servicio.

- Documentación técnica (oficial) con las características de las soluciones desplegadas, manuales técnicos y operativos, etc
- Otros Entregables: Otra documentación que pueda complementar a la anterior (Plan de Calidad,…).

La documentación deberá mantenerse actualizada con la evolución del servicio (mejoras introducidas, nuevas políticas,…)

4.1.6 Transferencia de conocimiento

Como criterio general, durante la ejecución de los trabajos objeto de la contratación, el adjudicatario se compromete a facilitar en todo momento a EJIE/OSAKIDETZA y, si es el caso, a las personas designadas por esta a tales efectos, la información y documentación que estas soliciten para disponer de un pleno conocimiento de las circunstancias en que se desarrollan los trabajos, así como de los eventuales problemas que puedan presentarse y de las tecnologías, métodos y herramientas utilizados para resolverlos.

Adicionalmente, el adjudicatario deberá considerar los servicios necesarios para realizar la transferencia de conocimiento a EJIE/OSAKIDETZA. Las sesiones de transferencia de conocimiento comprenderán, al menos, los siguientes contenidos:

- Descripción técnica y de detalle sobre la solución implantada, así como del conjunto de elementos instalados y que forman parte de la solución de seguridad de los centros.
- Gestión y operación del servicio: monitorización, configuración del servicio, diagnóstico de averías, datos de uso del servicio, utilización plataformas centrales.

La transferencia de conocimiento deberá garantizar que el equipo de soporte de EJIE/OSAKIDETZA adquiera un completo conocimiento, tanto a nivel operativo como de configuración y manejo de la tecnología, que les permita hacer frente a las incidencias, cambios, etc. que puedan producirse en el sistema tras la migración.

Las sesiones de transferencia de conocimiento deberán ser impartidas, en la modalidad que EJIE/OSAKIDETZA consideren oportuna, por personal cualificado que cuente con un amplio conocimiento sobre las tecnologías involucradas en este contrato. La duración de las sesiones deberá ser, como mínimo, de:

- La transferencia de conocimiento deberá tener una duración mínima de veinte (20) horas, distribuidas en las sesiones que EJIE estime necesarias para adaptarse a la disponibilidad del personal de EJIE.

EJIE se reservará el derecho de pedir toda la formación o parte de ella al inicio del contrato que permita disponer del conocimiento necesario para hacer frente al mantenimiento de los equipos por parte de su equipo de soporte (Nivel 2) una vez recepcionados.

El adjudicatario deberá entregar manuales y documentación relativa a los temas tratados en las diferentes sesiones de transferencia de formación.

4.1.7 Recepción provisional de las instalaciones en centros

Para la recepción provisional de cada uno de los centros sanitarios se deberá cumplir lo siguiente:

- Validación por parte de EJIE/Osakidetza de la instalación realizada.
- Verificación por parte de EJIE/Osakidetza del correcto funcionamiento del servicio.
- Entrega y validación por parte de EJIE/Osakidetza del conjunto de la documentación as-built asociada a cada uno de los centros.
- Haber realizado las sesiones correspondiente a la transferencia de conocimiento, bajo las condiciones descritas en el apartado 4.1.6 del presente pliego.

En caso de incumplimiento sobre las condiciones de ejecución de instalaciones o bien los resultados de pruebas de servicio, seguridad, gestión remota, etc., el adjudicatario deberá proceder con las subsanaciones correspondientes, en un plazo máximo de quince (15) días hábiles, en las condiciones indicadas en el presente pliego, para considerar la validación de la instalación y entrega del servicio.

Asimismo, no se considerará finalizada la instalación, ni la entrega del servicio de un centro hasta que el adjudicatario no haya proporcionado toda la documentación requerida, y ésta haya quedado validada por EJIE.

La documentación as-built deberá ser entregada en un plazo máximo de dos semanas, tras la realización de la instalación y validación del funcionamiento del servicio en las condiciones requeridas en el presente pliego.

4.1.8 Operación y Explotación

El adjudicatario deberá proveer el soporte adecuado para la operación y explotación de los servicios en los centros que se vayan desplegando. El adjudicatario se hará responsable del mantenimiento y resolución de todas las incidencias y peticiones asociadas a la nueva infraestructura de seguridad desplegada, desde que se despliegue, hasta una (1) semana después de la recepción provisional del centro, momento a partir del cual su gestión será entregada al equipo de Operación y Soporte de EJIE (Nivel 2).

Finalizado el plazo de estabilidad del sistema definido (1 semana), en caso de que el Nivel 2 no pudiera resolver las incidencias registradas, éstas se derivarán inmediatamente al adjudicatario para su resolución, ya sea con medios propios o escalándolas al soporte técnico especializado experto de fabricante (Nivel 3) que también forma parte del alcance de este expediente.

4.2 Servicios de Ajuste y acondicionamiento del servicio

Una vez superada la fase de puesta en marcha, a lo largo de la duración del contrato, en respuesta a la estrategia de Osakidetza en materia de comunicaciones y seguridad corporativa y en coordinación con otros proyectos, será necesario realizar una serie de trabajos de ajuste y acondicionamiento del servicio, entre los que destacan:

- Replanteos en los diferentes centros sanitarios con objeto de analizar la situación de la instalación inicial y preparar un acondicionamiento de la misma. Se puede dar el caso de que en el momento de la puesta en marcha no exista una ubicación adecuada para el equipamiento, que el equipamiento no pueda ser conectado a los switches definitivos u otras situaciones que no permitan, en primera instancia, dejar la instalación en su estado definitivo.
- Trabajos en los diferentes centros sanitarios, en las mismas condiciones ya explicadas en el apartado 4.1, para ajustar la instalación inicial. Pueden ser necesarias operaciones como enrackado de equipos en nuevos armarios, reconexión de equipamiento a nuevos switches, u otras operaciones en el ámbito de un acondicionamiento de la instalación física.
- Trabajos de consultoría para la definición y aplicación de un nuevo modelo de segmentación y seguridad de red corporativo en Osakidetza. Como se ha comentado previamente en la actualidad no existe una segmentación efectiva, por lo que se pretende, en esta fase, llevar a cabo una redefinición del modelo de segmentación de red corporativo.

- Trabajos de resegmentación lógica de la red y aplicación de configuraciones en base a plantillas comunes en los Firewall de los centros sanitarios. Se trata de la aplicación del modelo expuesto en el punto anterio, lo cual supondrá operaciones lógicas en los Firewalls.

En esta fase la operación y explotación del equipamiento estará siendo realizada por el Soporte de Seguridad de EJIE (Nivel 2), por lo que todas las operaciones serán coordinadas con EJIE y con el Nivel 2.

En el momento en que el licitador tenga que realizar operaciones reconfiguración sobre los diferentes equipos, volverá a hacerse responsable del equipamiento, debiendo atender a las incidencias que puedan surgir como consecuencia de estas actuaciones hasta que el centro se de por entregado de nuevo a operación, siguiendo las mismas condiciones establecidas en los apartados 4.1.7 y 4.1.8

El licitador deberá ajustar también la documentación en consonancia con los ajustes realizados en los diferentes centros sanitarios.

4.3 Servicios de Mantenimiento (Nivel 3)

En este apartado, se indica el alcance de los servicios de mantenimiento (Nivel 3) solicitados a través del presente expediente. Además del servicio propio del fabricante, durante el periodo de garantía ofertado, el contratista adjudicatario se responsabilizará de servicios de mantenimiento adicionales de tercer nivel.

Estos servicios de mantenimiento se circunscriben a aquellos elementos adquiridos en el marco de este contrato y también se describen los acuerdos de nivel de servicio que deberá de prestar el adjudicatario del expediente y las penalizaciones a aplicar por incumplimiento.

Asimismo, y de acuerdo a lo especificado en capítulos previos, el adjudicatario deberá presentar informes mensuales de servicio con el objetivo de valorar el correcto cumplimiento de los SLAs acordados.

Con el fin de proporcionar correctamente los servicios objeto del contrato, el adjudicatario dispondrá de los acuerdos y contratos de soporte y mantenimiento necesarios con el fabricante.

En caso de modificaciones en la distribución geográfica de los elementos objeto de este contrato, el adjudicatario deberá asumir los cambios que se produzcan en este ámbito (siempre dentro de la CAPV) sin modificar el coste asociado a la prestación del servicio.

Mientras el contrato esté en vigor, el adjudicatario se responsabilizará de la gestión de todas las relaciones con el fabricante: apertura de casos de soporte, incidencias.

EJIE dispone de soportes adicionales denominados de segundo nivel (Nivel 2) que serán los encargados de facilitar el acceso a los elementos incluidos en contrato. Para todas actividades en el marco de este contrato que así lo requieran, dicho acceso será siempre a través de estos soportes de segundo nivel de EJIE no existiendo accesos remotos permanentes.

Así mismo, durante este periodo, EJIE tendrá la posibilidad, si así lo requiere, de realizar la apertura de casos y gestiones directamente con el fabricante a través de sus equipos de soporte Nivel 2, con objeto de reducir los tiempos de respuesta. En este sentido, el adjudicatario deberá habilitar los procedimientos necesarios para esta gestión (cambios de titularidad o cualquier otra modificación necesaria para este fin).

4.3.1 Servicio de Mantenimiento Correctivo

Para la resolución de incidencias (in situ o en remoto) generadas por problemas o mal funcionamiento de los elementos incluidos en contrato, incluyendo las tareas necesarias hasta conseguir la restauración del servicio y otras asociadas a la gestión de incidencias y mejora continua, como pueden ser:

- Coordinación con los grupos de soporte y resto de proveedores que conforman la solución.
- Administración de los sistemas objeto del contrato y de los servicios ofrecidos a través de estos sistemas.
- Trabajos de reconfiguración de elementos.
- Reparación y/o sustitución de elementos averiados.
- Instalación/desinstalación de elementos, según necesidad.
- Instalación de software por fallo, vulnerabilidades publicadas, necesidad de actualización detectada en el mantenimiento preventivo o por indicación del fabricante.
- Pruebas para verificación de la reposición del servicio.
- Escalado a fabricante.
- Soporte técnico avanzado propio y soporte especializado experto de fabricante en el ámbito de la incidencia.
- Registro, seguimiento y documentación de la incidencia hasta su resolución.
- Elaboración de informes o partes de intervención o averías, a petición de EJIE.

4.3.1.1 Acuerdos de Nivel de Servicio

El adjudicatario proporcionará soporte técnico avanzado con técnicos cualificados y soporte especializado experto de fabricante a través de los canales habituales: correo, web, teléfono y presencial. En este sentido, es necesario cumplimentar el apartado “Medios materiales” del Anexo II: Compromiso de adscripción de

medios incluido en el pliego de condiciones particulares con la información relativa al flujo y canales de comunicación.

Durante el periodo objeto de contratación, el adjudicatario se comprometerá a ser el punto de contacto para atender cualquier tipo de incidencia o consulta técnica que pueda surgir en los equipos objeto del contrato y actuar como intermediario en el escalado al soporte técnico especializado experto de fabricante, es decir, asumir labores de gestión, coordinación e interlocución con los soportes adicionales con los que EJIE cuenta y/o a su vez con el fabricante en el caso de incidencias, actualizaciones de software, consultas y demás circunstancias posibles.

A continuación, se especifican diferentes niveles de servicio requeridos en la prestación del servicio de mantenimiento correctivo:

- Horario de prestación del servicio: 24x7. El adjudicatario deberá disponer tanto de un soporte propio 24x7 como del mantenimiento necesario con el fabricante. Se deberá acreditar la disposición de ambos servicios y que los perfiles profesionales asignados tengan autorización en la apertura de incidentes directamente con el fabricante.
- Devolución del equipo averiado, ya reparado: entrega al siguiente día hábil. El adjudicatario deberá disponer del contrato de soporte necesario para abrir una incidencia al fabricante y agilizar mediante las pruebas oportunas la autorización del RMA. En el caso de RMAs, la empresa adjudicataria correrá además con todos los gastos de logística derivados de los mismos.
- Con el fin de cumplir los acuerdos de nivel de servicio, el adjudicatario dispondrá de los acuerdos y contratos de soporte y mantenimiento necesarios con el fabricante, de los cuales aportará los correspondientes certificados del fabricante donde se especificará el detalle de base instalada cubierta.
- Se deben cumplir los siguientes tiempos de respuesta y resolución según la siguiente clasificación:
    - Críticas y graves: incidencias en el equipamiento que impidan o degraden el uso del servicio, resultando en incidencias por parte de la persona usuaria final.
    - Leves: incidencias que no impiden el funcionamiento del servicio, pero que degradan su uso de manera leve, sin suponer incidencias de la persona usuaria final.
    - Consultas: consultas técnicas en el ámbito de las tecnologías especificadas.

La siguiente tabla muestra los tiempos máximos a cumplir por el adjudicatario:

	Críticas y graves	Leves	Consultas

Tiempos de respuesta	15 minutos	15 minutos	-
Tiempos de resolución	4 horas (restauración servicio)	24 horas	96 horas

- Devolución del equipo averiado, ya reparado: entrega al siguiente día hábil. El adjudicatario deberá disponer del contrato de soporte necesario para abrir una incidencia al fabricante y agilizar mediante las pruebas oportunas la autorización del RMA.

Con el fin de cumplir los acuerdos de nivel de servicio, el adjudicatario dispondrá de los acuerdos y contratos de soporte y mantenimiento necesarios con el fabricante, de los cuales aportará los correspondientes certificados del fabricante donde se especificará el detalle de base instalada cubierta.

La notificación de las diferentes averías al adjudicatario correspondiente se realizará por personal de EJIE o por los soportes con los que EJIE cuenta. Teniendo en cuenta lo anterior, se definen los siguientes conceptos:

- Tiempo de respuesta: tiempo transcurrido desde la comunicación de la avería hasta el inicio de las actividades encaminadas a su resolución.

- Tiempo de resolución: tiempo transcurrido desde la comunicación de la avería hasta el restablecimiento del servicio.

En cualquier caso, deberán entregarse informes mensuales de servicio y cumplimiento de SLAs.

4.3.2 Servicio de Mantenimiento Preventivo

Se realizarán propuestas orientadas a mejorar el rendimiento y/o disponibilidad del Servicio. Se incluye la propuesta de la línea base de monitorización para una detección temprana de problemas, el análisis de las versiones software y estado del servicio buscando el reducir el número de incidencias a futuro en la red, la revisión de obsolescencia tecnológica y fechas de fin de vida, y el health check de la infraestructura para revisar la salud y configuraciones.

Se considerará que aporta valor el tener soporte directo de fabricante para revisiones periódicas de la plataforma, recomendaciones, conocimiento de nuevas funcionalidades y roadmap previsto, así como para otro tipo de tareas de Mantenimiento Preventivo que permitan sacar el máximo partido a la Plataforma a todos los niveles.

4.3.2.1 Acuerdos de Nivel de Servicio

A continuación, se indican los requisitos relativos a los acuerdos de nivel de servicio en el mantenimiento preventivo que serán de aplicación.

El licitador a partir de inspecciones y/o mediciones periódicas (como mínimo 2 anuales) debe realizar propuestas orientadas a mejorar el rendimiento y/o disponibilidad de la red, incluyendo:

- Propuesta de la línea base de monitorización para una detección temprana de problemas.
- Análisis de las versiones software y estado del servicio buscando el reducir el número de incidencias a futuro.
- Revisión obsolescencia tecnológica y fechas de fin de vida.
- Health check de la infraestructura para revisar la salud y configuraciones, aplicación de las best practices y las recomendaciones particularizadas a nuestro entorno.

En los informes preventivos, como mínimo dos, uno a final del primer trimestre y otro a final del tercer trimestre, deben de reflejarse las acciones sobre el hardware/software que se consideren necesarias:

- Propuesta.
- Ventajas/inconvenientes de la nueva plataforma.
- Estimación de esfuerzo e impacto sobre el servicio.
- Observaciones si las hubiera.

4.3.3 Servicios de Mantenimiento Adicionales de Tercer Nivel del Adjudicatario

- Alta de las garantías del hardware, software y de la suscripción de las licencias. Se darán de alta las garantías del hardware, software y la suscripción de las licencias objeto de contrato hasta el periodo de validez del contrato indicado. Todas las altas y mantenimientos deberán ser oficiales y estar garantizadas por el fabricante.

- Renovación de la suscripción de las licencias. Se renovará la suscripción de las licencias objeto de contrato de acuerdo con los planteamientos indicados en este pliego de condiciones. Todas las renovaciones y mantenimientos deberán ser oficiales y estar garantizadas por el fabricante.

- Asunción de evoluciones sobre la misma plataforma. Si durante la vigencia del contrato, se decidiera actualizar o evolucionar los servicios existentes, el adjudicatario deberá asumir el mantenimiento de esas posibles evoluciones sobre la misma plataforma objeto del presente contrato.

- Intervenciones planificadas. Las operaciones y asistencias que requieran los servicios descritos, por ejemplo, la parada de algún elemento que conforma la plataforma o de alguno de los servicios que presta, se planificarán de acuerdo con el personal técnico de EJIE en un horario convenido y que menos afecte al funcionamiento de dichos servicios.

- Estadísticas de uso de la plataforma. EJIE podrá solicitar al adjudicatario la elaboración de un informe con toda la información relativa al servicio que la plataforma presta. EJIE validará y podrá a su vez requerir la inclusión de más información en el citado informe.

4.3.4 Otros Requisitos Asociados a la Prestación del Servicio de Mantenimiento

4.3.4.1 Stock de Productos

El adjudicatario podrá disponer de los elementos hardware y software de respaldo que considere necesario para asegurar los niveles de servicio comprometidos.

4.3.4.2 Medios Técnicos y Herramientas de Apoyo al Servicio

Todo el material técnico necesario para posibilitar la prestación del servicio, de acuerdo al alcance y requisitos solicitados, será responsabilidad del adjudicatario, quedando EJIE exento de cualquier obligación de suministrar dichos elementos.

La empresa adjudicataria deberá disponer de las herramientas adecuadas para el registro de las incidencias y peticiones solicitadas con relación al servicio, documentación de actuaciones para su resolución y medición de los niveles de servicio solicitados.

Asimismo, el adjudicatario debe garantizar la adecuada integración de sus servicios de atención técnica con los servicios de atención técnica establecidos por EJIE, debiendo hacer uso de las plataformas de gestión y mantenimiento del servicio dispuestas por EJIE y ajustando sus procedimientos, si EJIE así lo solicitara.

4.3.5 Problemáticas de rendimiento y/o funcionamiento identificadas durante el período de vigencia del contrato

El adjudicatario deberá cumplir con los requerimientos, funcionalidades y rendimientos indicados como de obligado cumplimiento en el presente expediente.

En caso de que durante la vigencia del contrato se identifiquen problemas de rendimiento o no cumplimiento de alguna de las funcionalidades solicitadas, y que sean imputables al adjudicatario, éste deberá realizar los suministros y actualizaciones de equipamiento Hardware o Software que sean necesarios para cumplir con el objeto del contrato, estableciéndose para ello un período máximo de 6 meses, superado el cual EJIE podrá optar por la rescisión del contrato.

Asimismo, durante el proceso de instalación y mantenimiento, se aplicarán las penalizaciones definidas en el Pliego de clausulas administrativas (PCP) correspondiente a la presente licitación.

4.3.6 Garantía, soporte y mantenimiento

El adjudicatario contraerá el compromiso formal, que deberá asumir de un modo expreso, de garantizar todos y cada uno de los suministros e instalaciones a realizar contra toda clase de defectos de material empleado.

El adjudicatario deberá incluir junto con los suministros (Hardware, Software y Licencias), la garantía y soporte de fabricante de acuerdo con las siguientes condiciones:

- Todos los elementos objeto de suministro deberán disponer de garantía de fabricante a lo largo de la duración del contrato.
- Se incluye el software y licencias necesario para garantizar las diferentes funcionalidades y tecnologías propuestas, incluyendo su mantenimiento.
- El hardware suministrado por la empresa adjudicataria deberá incorporar la última versión de microcódigo, firmware o software recomendada por el fabricante.
- Todos los materiales que suministrará la empresa adjudicataria, como parte de la ejecución de este contrato, deberán ser necesariamente nuevos, no admitiéndose equipos usados, ni total o parcialmente reparados o reconstruidos.
- Se incluyen las actualizaciones derivadas de la evolución tecnológica de las plataformas.
- El soporte de fabricante deberá incluir el acceso a las actualizaciones de firmware, parches, alertas de seguridad, y nuevas versiones de software durante el periodo de garantía de todo el equipamiento que se adquiere sin coste adicional. El suministro de la actualización incluirá tanto los productos como la documentación asociada.
- El soporte y mantenimiento deberán cumplir con los niveles de servicio establecidos en el presente pliego.

- El adjudicatario deberá disponer de los acuerdos y contratos de soporte y mantenimiento necesarios con el fabricante, de los cuales aportará los correspondientes certificados del fabricante donde se especificará el detalle de base instalada cubierta.
- Durante el periodo de garantía, el adjudicatario se responsabilizará de la gestión de todas las relaciones con el fabricante: apertura de casos de soporte, incidencias, RMAs relacionados con los equipos suministrados en el presente pliego. En el caso de RMAs, el adjudicatario correrá con todos los gastos de logística derivados de los mismos.

Así mismo, como se ha comentado previamente, el adjudicatario se hará responsable del mantenimiento y resolución de todas las incidencias asociadas a la nueva infraestructura de seguridad desplegada, desde que queda operativa, hasta una (1) semana después de la recepción provisional del centro, momento a partir del cual su gestión será entregada al equipo de Operación y Soporte de EJIE.

Finalizado el plazo de estabilidad del sistema definido (1 semana), en caso de que el Nivel 2 no pudiera resolver las incidencias registradas, éstas se derivarán inmediatamente al adjudicatario para su resolución, ya sea con medios propios o escalándolas al soporte técnico especializado experto de fabricante (Nivel 3) que también forma parte del alcance de este expediente.

El objetivo principal del adjudicatario será el de asegurar la restauración de la operación normal del servicio tan rápido como sea posible y mantener los mejores niveles de calidad y disponibilidad del servicio.

El licitador deberá incluir en su oferta la reposición del hardware en Next Business Day (NBD).

Los licitadores deberán presentar un documento con la descripción de los Procedimientos vinculados a la Gestión del Soporte de fabricante y Garantías (gestión RMA) del equipamiento suministrado para el periodo en cuestión, teniendo en cuenta los niveles de servicio solicitados en cada caso.

Para la ejecución de las labores de mantenimiento por parte del adjudicatario, EJIE facilitará el acceso a los equipos alcance del presente contrato a través de su soporte de segundo nivel. Para todas las actividades en el marco de este contrato que así lo requieran, dicho acceso será siempre a través de estos soportes de segundo nivel de EJIE no existiendo accesos remotos permanentes.

4.4 Requisitos asociados a los servicios

4.4.1 Plazos Parciales de Ejecución

A continuación, se presentan los hitos y plazos relevantes con relación a la duración y vigencia del contrato, que tiene una duración de 5 años:

- Los Servicios de Puesta en Marcha descritos en el apartado 4.1 deben estar finalizados antes del 31/12/2023, siendo este un requisito asociado a los Fondos Europeos para el Plan de Recuperación, Transformación y Resiliencia.

Este plazo condiciona de forma significativa la velocidad de despliegue necesaria y, por lo tanto, el número de recursos necesarios para la ejecución de esta fase. Además esta fase se ve condicionada por el plazo de suministro proporcionado por el fabricante, debiendo existir un compromiso firmado por parte del mismo, tal y como se establecerá en el PCP.

- Los Servicios de Ajuste y Acondicionamiento del servicio descritos en el apartado 4.2 se prestarán a partir del 1/1/2024, pudiendo recurrir a ellos hasta el final del contrato (5 años de duración).
- Los Servicios de Mantenimiento (Nivel 3) del integrador según apartado 4.3 se prestarán a lo largo de todo el contrato (5 años de duración).

Se refleja en el siguiente esquema los plazos e hitos asociados a los diferentes servicios:



4.4.2 Requisitos Generales

Los trabajos a desarrollar por el adjudicatario se consideran "llave en mano", por lo que éste deberá aportar todas las prestaciones, suministros y servicios que sean necesarios, excepto aquellos que de forma explícita se hayan establecido como fuera del alcance del contrato. Ello incluye la puesta a disposición del personal técnico adecuado y con la experiencia necesaria para la prestación de los servicios.

Asimismo, el adjudicatario aportará todas las herramientas, aparatos, equipos de medida/pruebas, y cualquier otro material que pueda ser necesario para llevar a cabo las tareas requeridas para la ejecución del contrato.

En el desarrollo de los trabajos objeto del servicio es responsabilidad del adjudicatario atenerse a toda la normativa que sea de obligado cumplimiento y a la buena práctica que en cada momento sea aplicable a la actividad que realiza, tanto en sus aspectos técnicos como administrativos.

Serán por cuenta del adjudicatario los seguros necesarios para la realización de las actividades objeto del presente pliego, así como para cubrir los posibles daños o perjuicios que pudieran ocasionarse.

Como criterio general, durante la ejecución de los trabajos objeto de la contratación, la empresa adjudicataria se compromete a facilitar en todo momento a EJIE y, si es el caso, a las personas designadas por esta, la información y documentación que estas soliciten para disponer de un pleno conocimiento de las circunstancias en que se desarrollan los trabajos, así como de los eventuales problemas que puedan presentarse y de las tecnologías, métodos y herramientas utilizados para resolverlos.

En ningún caso el adjudicatario podrá realizar acciones de comunicación y/o difusión del proyecto sin la debida autorización previa por parte de EJIE.

4.4.3 Seguimiento y control de la ejecución del proyecto

4.4.4 Coordinación global del proyecto

EJIE será responsable de la gestión y seguimiento global del proyecto, velando por el cumplimiento de hitos y objetivos establecidos en contrato. Entre las tareas a realizar, se incluye:

- Gestión y seguimiento global del proyecto, velando por el cumplimiento de hitos y objetivos establecidos en contrato.
- Establecimiento, en colaboración con el adjudicatario, del conjunto de metodologías y procedimientos necesarios, que garanticen las actuaciones coordinadas y faciliten el cumplimiento de planificación.
- Validación de la solución y de las instalaciones, a través de las siguientes acciones:
    - Definición preliminar de los criterios de diseño y condiciones de ejecución de los diferentes trabajos.
    - Validación del diseño final de la solución.
    - Revisión y validación del Plan de Implantación que se adopte al despliegue según las necesidades identificadas a cada centro sanitario, si aplica.
    - Revisión y validación de la documentación de acuerdo con las condiciones y criterios previos establecidos.
    - Supervisión de trabajos y Auditorías in situ en un porcentaje de centros, dando el visto bueno a las ejecuciones y solicitando las subsanaciones cuando procedan.
    - Coordinación principal de EJIE y adjudicatarias de los soportes y otros agentes (entidad) que estén involucrados/afectados en/con la ejecución de los trabajos.
    - Validación de la documentación final correspondiente a cada instalación (proyectos finales, pruebas...), con especial hincapié en los resultados de pruebas para la migración.
    - Planificación de reuniones de seguimiento del proyecto.
    - Verificación de cumplimiento de las condiciones para la entrega a Operación.

Validación del resto de documentación as-built, como son las actas de entrega de material y tablas de inventario, para poder establecer el cierre de proyecto.

4.4.5 Control de ejecución por parte del adjudicatario

Si bien la gestión y dirección global del proyecto será llevada a cabo por parte de EJIE, **el adjudicatario será el responsable principal de controlar la ejecución de los trabajos**, estableciendo para ello, todos los mecanismo y procedimientos necesarios que garanticen el cumplimiento de la planificación, la correcta operatividad de la solución y la calidad en el servicio final.

Uno de los aspectos más críticos del proceso de implantación y puesta en marcha es la necesidad de coordinación de los trabajos con los siguientes agentes para que la instalación de la infraestructura de seguridad se realice con éxito y mínimo impacto posible:

- Osakidetza
- EJIE
- Los diferentes Proveedores, que EJIE considere

El adjudicatario designará un Jefe de Proyecto como interlocutor principal con EJIE para el control de ejecución del proyecto que tendrá una participación activa en lo relativo a la prestación de los servicios de puesta en marcha y mantenimiento de la solución.

El Jefe de Proyecto se responsabilizará de las siguientes tareas principales:

- Realizará la coordinación y seguimiento continuo de la evolución de los trabajos y velará por mantener el plan de ejecución de trabajos periódicamente actualizado, considerando en todo momento la integración de sus tareas (validación de diseños, validación replanteos y planes de trabajo, pruebas, etc.) con aquellas que involucren a EJIE (y soportes).
- Será el responsable por parte del adjudicatario de disponer de los medios necesarios y organizar los recursos y equipo de trabajo para garantizar el cumplimiento del plan, y definirá metodologías para control de riesgos y definición de propuestas de mitigación de los mismos que garanticen los resultados esperados en proyecto en plazos y calidad técnica.
- Organizará el conjunto de recursos necesarios para la ejecución de los trabajos de instalación siempre con el objetivo de cumplir la planificación definida.
- Podrá tener, a consideración de EJIE, interlocución directa con otros involucrados del proyecto por parte de EJIE como son los grupos de soporte.
- Realizará reportes de avance de proyecto.
- Definirá metodologías para identificación y control de riesgos y definición de propuestas de mitigación de estos.

- Asistirá, junto con los técnicos que se estime conveniente, a las reuniones de seguimiento y técnicas que convoque EJIE, y con la periodicidad que se designe.
- Garantizará que toda la información y documentación del proyecto se encuentra en todo momento actualizada en la plataforma de gestión que a tal efecto disponga EJIE (planificaciones, informes de replanteo, documentos técnicos, documentos de inventario, proyectos finales, etc.).
- Realizará el seguimiento periódico sobre la calidad de los servicios de mantenimiento solicitados y será el responsable de garantizar el cumplimiento de los acuerdos de nivel de servicio asociados.

4.4.6 Gestión documental

Para el seguimiento del proyecto, EJIE pondrá a disposición del adjudicatario una **plataforma de gestión documental**, accesible a todos los usuarios autorizados, y donde se mantendrá actualizada de forma diaria la documentación del proyecto. Esta herramienta será de especial relevancia principalmente como herramienta de información sobre los avances de proyecto, y herramienta de intercambio para la validación de la documentación de proyecto durante la ejecución del contrato.

El adjudicatario y EJIE deberán interactuar directamente contra la Plataforma de gestión indicada, siendo el adjudicatario el responsable del registro y volcado de la documentación que se vaya generando, que puede ser por ejemplo:

- Datos de partida (listados de centros, equipos, etc.).
- Documentos sobre el diseño de la solución y plan de actuación.
- Criterios y acuerdos relativos a la ejecución de los trabajos e instalaciones en centros.
- Documentación solicitada por Operación.
- Planificación del proyecto:
    - ✓ Planificación acordada (cerrada) de actuaciones particulares en centros sanitarios (despliegues, instalaciones, pruebas, etc.).
    - ✓ Informe completo de los avances de despliegue de cada centro sanitario
- Proyectos finales incluyendo los resultados de las instalaciones realizadas y las pruebas en centros sanitarios.
- Documentación de inventario y actas de entrega de material/servicio en centros sanitarios.
- Cuadros de Mando de carácter ejecutivo para control de avance del despliegue y control sobre las necesidades de materiales.

La plataforma podrá albergar otra documentación adicional que se vaya generando de forma conjunta durante la ejecución del proyecto, como puede ser:

- Procedimientos y metodologías de trabajo acordados entre los grupos implicados en la puesta en marcha del servicio (adjudicatario, soportes, etc.)
- Criterios de diseño y condiciones de ejecución de instalación.
- Procedimientos para la atención de incidencias y defectos durante el despliegue y antes de la entrega a operación y/o aceptación del centro.

El adjudicatario deberá obligatoriamente garantizar la disponibilidad y actualización de la documentación indicada en el presente documento.

4.4.7 Reuniones de seguimiento

Para el seguimiento y control del contrato, EJIE convocará reuniones de seguimiento con la periodicidad que ésta designe, pudiendo requerir que sea en sus oficinas, destinadas a validar de forma continuada el cumplimiento de los objetivos especificados, tanto en plazos como en términos de calidad final.

4.5 Equipo de trabajo

El equipo de trabajo propuesto por el adjudicatario deberá estar formado por personal técnico con categoría profesional y nivel de especialización adecuados a las necesidades planteadas en el presente pliego.

El equipo de trabajo del adjudicatario estará dirigido por un **Jefe de Proyecto** que deberá contar con disponibilidad para atender sin demora los requerimientos de los responsables designados por EJIE. El responsable del proyecto deberá contar con capacidad suficiente para tomar las decisiones que se adopten sobre las prestaciones contratadas sin que estas puedan verse afectadas por la falta de capacidad decisoria, ya sea legal o formal. Este Delegado será el único interlocutor principal con la Dirección del Proyecto de EJIE. Dispondrá de teléfono móvil, para facilitar su localización, y correo electrónico

El dimensionamiento del equipo deberá realizarse acorde a la metodología planteada por el licitador, a los tiempos y planificaciones establecidas y a los requerimientos mínimos expuestos en el presente pliego.

En cualquier caso, el adjudicatario será el responsable de garantizar los medios durante la ejecución del proyecto y éstos deberán adecuarse en todo momento para cumplimiento de los hitos y plazos establecidos.

Un aspecto clave para el dimensionamiento de recursos y organización es, no solo la ejecución de los trabajos en centros, sino también la necesidad de elaboración de documentación (informes finales, inventarios, documentación de entrega a Operación, actas de servicio…) requerida en las diferentes fases de proyecto. Todo ello puede suponer un cuello de botella al adjudicatario si éste no realiza el dimensionamiento adecuado de la Oficina Técnica destinada a la ejecución de estos trabajos.

Asimismo, en el inicio del proyecto, el adjudicatario deberá exponer la relación detallada del equipo de trabajo propuesto y dedicaciones. EJIE podrá solicitar cambios sobre los recursos propuestos en caso de que, tras el análisis de la propuesta, determine que los medios propuestos no son suficientes y/o adecuados para el cumplimiento del plan de trabajo.

Los posibles inconvenientes de adaptación al entorno de trabajo y al proyecto debidos a las sustituciones de personal, deberán subsanarse mediante periodos de solapamiento sin coste adicional, durante el tiempo necesario. Si a criterio de la Dirección del Proyecto de EJIE, esto no fuera posible, las dos primeras semanas de trabajo del sustituto/s no serán facturables corriendo a cargo del adjudicatario.

Los componentes del grupo de trabajo desarrollarán su labor con hardware y software propiedad del adjudicatario.

El dimensionamiento del equipo de trabajo deberá realizarse considerando el tiempo necesario para la ejecución de las instalaciones en cada uno de los centros sanitarios alcance del contrato y las propias operaciones que, en algún caso, pueden requerir de al menos 2 personas (enrackado de grandes equipos). El dimensionamiento y dedicación final de estos recursos estará sujeto a la organización del proyecto por parte del adjudicatario para cumplimiento de los plazos previstos.

A fin de evitar riesgos de afectación al servicio por la posible indisponibilidad de los equipos que componen la actual infraestructura de seguridad, se considera de suma importancia que el adjudicatario defina las necesidades mínimas, en lo que a disponibilidad y dedicación de los recursos humanos se refiere, para asegurar el cumplimiento de los plazos de instalación.

El adjudicatario pondrá a disposición el personal técnico adecuado con la preparación y experiencia necesarias, con el dimensionamiento y dedicaciones requeridas, para llevar a cabo las tareas requeridas para la ejecución del contrato.

A continuación, se especifican los roles mínimos identificados a los que deberá dar respuesta el adjudicatario para la ejecución del presente contrato, y que se acompañarán del equipo de trabajo necesario para la ejecución de los trabajos solicitados en los plazos requeridos:

- **Jefe/a o Director/a de Proyecto,** mencionado previamente**,** que será el responsable último del contrato y de la disposición de los medios y su coordinación para cumplimiento de los objetivos del proyecto (plazos, calidad, alcance...), y con los conocimientos y capacidades solicitados en el PCP.
- **Oficina Técnica Adjudicatario:** formada por al menos los siguientes perfiles especialistas a los que de forma obligatoria deberá dar respuesta el adjudicatario para garantizar la calidad técnica del proyecto, tanto en la fase de Puesta en Marcha inicial como en la fase de Ajuste y Acondicionamiento del Servicio posterior, no teniendo por qué dedicar todos los recursos en esta última fase:
- **Especialista en tecnología del fabricante de la tecnología ofertada para este expediente para el diseño y migración,** que será el responsable técnico del diseño de la solución, plan de migración y construcción del nuevo entorno, y con los conocimientos y capacidades solicitados en el PCP.

- **<u>Equipo de despliegue:</u>**
    - Un ***Coordinador de los recursos*** *de despliegue,* necesario como consecuencia del elevado número de recursos de instalación a destinar al proyecto.
    - **2 cuadrillas de instaladores y 2 adicionales de back-up** en caso de necesidad para recuperación de los ritmos de trabajo y aseguramiento del cumplimiento de los plazos establecidos. Se define como cuadrilla el número de personas necesarias para acometer los trabajos de desinstalación de los actuales equipos e instalación de los nuevos equipos que formarán parte de la nueva solución de seguridad de los centros pertenecientes a la Red de Osakidetza (en este sentido, una cuadrilla puede ser una o varias personas). Con este dimensionamiento de equipo de despliegue se pretende conseguir un ritmo de migración de centros tal que se puedan cumplir las fechas establecidas en este pliego

      A continuación se detalla las especificaciones de “cuadrilla” y su dimensionamiento:

      La migración en sede siempre requerirá de, mínimo:
        - Un recurso en sede
        - Un segundo recurso (no obligatoriamente en sede) que realice la conexión del nuevo equipo instalado con la gestión, carga de políticas, etc.
          Este segundo recurso puede ser compartido por varias cuadrillas

- **<u>Equipo para la prestación de los servicios de mantenimiento</u>,** adecuadamente dimensionado para la prestación de los servicios con los SLAs acordados y con los conocimientos y capacidades solicitados en el PCP

Dichos perfiles y su descripción deberán reflejarse en el Anexo II del PCP (anexo de adscripción de medios), justificando aquellos con requisitos en la fase de solvencia técnica.

El adjudicatario será el responsable de garantizar los medios durante la ejecución del proyecto y éstos deberán adecuarse en todo momento para cumplimiento de los hitos establecidos.

Con el inicio del proyecto, el adjudicatario deberá actualizar su plan de trabajo y exponer la relación detallada del equipo propuesto y dedicaciones en cada fase del proyecto. EJIE podrá solicitar cambios sobre los recursos expuestos en caso de que, tras el análisis de la propuesta, determine que los medios expuestos no son suficientes y/o adecuados para el cumplimiento de los planes de trabajo.

5 Anexos

5.1 Anexo I PCT_Checklist requisitos técnicos

Este anexo deberá ser completado por los licitadores y entregarse junto con la oferta técnica (Sobre C).