



Financiado por la Unión Europea
NextGenerationEU



GOBIERNO DE ESPAÑA
Plan de Recuperación,
Transformación y Resiliencia

EUSKO JAURLARITZA



GOBIERNO VASCO



Estado Jerárquico Informático Directo
Sistema Informático del Gobierno Vasco

Suministro para la Renovación de la Infraestructura de Seguridad y Control de Navegación del Departamento de Educación y servicios de migración y mantenimiento

Especificaciones de compra / Pliego de condiciones técnicas

Junio 2022



Este documento es propiedad de Eusko Jaurlaritzaren Informatika Elkarte – 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	03/06/2022	Versión Inicial	Josu Bagazgoitia	Aritza Iratzagorria



Índice

1	Introducción	5
2	Situación actual y necesidades	6
3	Objeto del contrato.....	8
4	Ámbito geográfico	9
5	Alcance del contrato	10
5.1	Suministro de equipamiento	10
5.2	Instalación, configuración, migración y puesta en marcha.....	11
5.3	Borrado de configuración y retirada de los equipos actuales.....	12
5.4	Seguimiento y control del proyecto.....	12
5.5	Operación y explotación	12
5.6	Garantía, soporte y mantenimiento	12
5.7	Inventario de elementos y documentación as-built	14
5.8	Stock para equipamiento en centro	16
6	Requisitos técnicos y funcionales	17
6.1	Arquitectura actual del sistema.....	17
6.2	Requisitos de diseño de la solución	19
6.3	Firewall Centros: Tipos, Cantidad y Rendimientos.....	20
6.3.1	Tipos y Cantidad	20
6.3.2	Rendimientos	21
6.4	Firewall Centros: Requisitos Networking	22
6.5	Firewall Centros: Requisitos Seguridad, VPN, Autenticación y Delegación.	23
6.6	Firewall Centros: Requisitos Control de Navegación a Internet.....	24
6.7	Requisitos Gestión, Logs y Reporting centralizado.....	25
6.8	Otros requisitos técnicos y funcionales	26
6.9	Checklist de requerimientos	27
7	Servicios Profesionales	28
7.1	Servicios de consultoría y diseño de la solución	28
7.2	Plan de migración para la convivencia de servicios	28
7.3	Servicios de instalación, configuración y puesta en marcha.....	29
7.4	Otros servicios de definición previos al despliegue.....	30
7.5	Mantenimiento del equipamiento.....	31
7.5.1	Mantenimiento correctivo. Acuerdos de nivel de servicio	31
7.5.2	Mantenimiento preventivo. Acuerdos de nivel de servicio	32
7.5.3	Stock de equipos	33
7.5.4	Medios técnicos y herramientas de apoyo al servicio	33
7.6	Transferencia de conocimientos a EJE	33
7.7	Garantía, soporte y mantenimiento de la solución.	34
7.7.1	Garantía, soporte y mantenimiento	34



7.7.2	Problemáticas de rendimiento y/o funcionamiento identificadas durante el período de vigencia del contrato.....	35
7.8	Recepción provisional de las instalaciones en centros	36
7.9	Seguimiento y control del proyecto.....	36
7.9.1	Coordinación global del proyecto	36
7.9.2	Control de ejecución por parte del adjudicatario	37
7.9.3	Gestión documental	37
7.9.4	Reuniones de seguimiento	38
7.10	Equipo de trabajo.....	38
8	Anexos.....	41
8.1	Anexo I PCT_Centros Educativos Red Premia	41
8.2	Anexo II PCT_Checklist requisitos técnicos	41
8.3	Anexo III PCT_ Índice diseño de la solución	41
8.4	Anexo IV PCT_ Plantilla CMDDB.....	41



1 Introducción

EJIE, Eusko Jaurlaritzaren Informatika Elkarte – 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 <https://www.ejie.eus>

En el Consejo de Gobierno de 14 de enero de 2014, el Consejero de Hacienda y Finanzas informó de una iniciativa departamental consistente en el inicio de un proyecto de estudio y análisis de las oportunidades de mejora derivadas del proceso de convergencia en materia de Tecnologías de la Información y de la Comunicación (TIC) en el seno de la Administración Pública y el sector público de la Comunidad Autónoma de Euskadi.

La labor consistía en definir un nuevo modelo basado en el análisis detallado de la situación actual de prestación de servicios en materia de Tecnologías de la Información y de la Comunicación (TIC) en el seno de la Administración Pública y el sector público de la Comunidad Autónoma de Euskadi, comprendiendo la Red Corporativa Administrativa del Gobierno Vasco y las Redes Sectoriales, así como cualquier otra infraestructura informática y de comunicaciones utilizada por las entidades del sector público de la Comunidad Autónoma de Euskadi.

La propuesta elaborada fue aprobada en Consejo de Gobierno de 27 de Julio de 2015, instando a llevar a cabo un proceso de convergencia en materia TIC en principio circunscrito a las infraestructuras y elementos anexos (Infraestructuras, Comunicaciones, Puesto de Trabajo y Servicios Corporativos Unificados), proponía una metodología y gobernanza de trabajo para la implementación del nuevo modelo de convergencia TIC-ICPS articulado a través de EJIE.

En Consejo de Gobierno de 21 de junio de 2016 se aprueba el documento ejecutivo «*Plan General de actuación en materia de Convergencia*» y se autoriza la implementación del proceso de convergencia, consistente en la puesta en marcha desde EJIE como órgano gestor de un Catálogo de Servicios ICPS a ofrecer a los Entes y Redes del Sector Público vasco y a implementar de forma paulatina.



2 Situación actual y necesidades

En 2015, EJE acometió un proyecto para la implementación de una solución de seguridad en Red PREMIA a fin de dotar a los centros educativos integrados en dicha red de servicios de seguridad LAN, servicios de control de navegación segura a Internet y servicios DHCP.

Actualmente, la Red PREMIA cuenta con un total de setecientos sesenta y cuatro (764) centros educativos, que cuentan con protección perimetral de red “Firewall” del fabricante Fortinet, disponiendo de una variedad de modelos en función del tamaño y fase de despliegue en las que se ha acometido la puesta en marcha de los equipos en los centros educativos.

Adicionalmente, se dispone de equipos centrales en los CPDs de EJE y LAKUA, así como de algunos equipos adicionales en STOCK y en centros asociados a servicios de soporte para disponer de entornos de pruebas similares a los centros educativos.

Así, a fecha de redacción del presente pliego se dispone del siguiente inventario de equipos:

Modelo equipo	Unidades	Fecha fin de vida hardware (EOL)	Fecha fin mantenimiento actual (Expedientes EJE: 066-2019 y 080-2021)	Fecha fin mantenimiento nuevo (Expediente EJE: 053-2022)
FortiGate-100D	624 + 7 (STOCK) = 631	26/07/2023	31/12/2022	26/07/2023 (EOL)
FortiGate-200D	87	22/05/2023	31/12/2022	22/05/2023 (EOL)
FortiGate-200E	2	05/09/2024	31/12/2022	31/12/2023
FortiGate-1500D	3 + 1 (STOCK) = 4	31/12/2026	31/12/2022	31/12/2026 (EOL)
FortiGate-60F	25 + 6 (STOCK)=31	No publicada	31/12/2022	31/12/2023
FortiGate-101F	26 + 4 (STOCK) = 30	No publicada	31/12/2022	31/12/2023
FortiAnalyzer-3000F	2	11/06/2023	31/12/2022	11/06/2023 (EOL)
FortiManager FMG	1	No aplica	31/12/2022	31/12/2023

Tabla 1: Inventario de equipos que conforman la infraestructura de seguridad del Departamento de Educación

De acuerdo con la tabla 1, hay que tener en cuenta varias consideraciones:

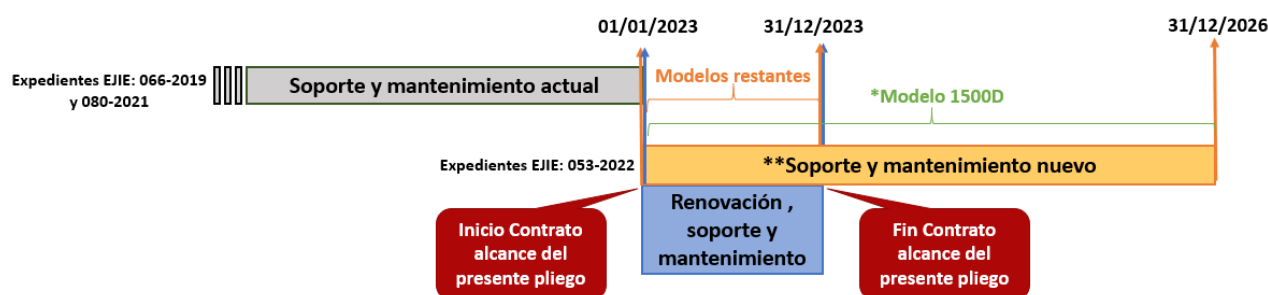
- Hay cuatro (4) modelos de equipo cuya fecha de fin de vida se encuentra próxima a su finalización (**mayo, junio y julio de 2023**):
 - ✓ A nivel de equipamiento en los centros, esta situación afecta aproximadamente un 93% del equipamiento.
 - ✓ A nivel de equipamiento central, esta situación afecta al 100% de la plataforma de reporting.
- Hay dos (2) modelos de equipo cuya fecha de fin de vida está sin publicar, que afecta aproximadamente al 7% de los centros educativos.
- Los Firewall centrales (modelo 1500D) tienen su EOL el 31/12/2026.



Teniendo en cuenta estas consideraciones, existe una necesidad de renovación tecnológica (hardware, software y licencias) de la solución, habiéndose optado por la siguiente estrategia de cara a proporcionar continuidad al servicio:

- Los Firewall centrales (modelo 1500D) se seguirán utilizando hasta su EOL el 31/12/2026. Esta decisión está basada en un criterio de protección de la inversión realizada. Tal y como se puede ver en la tabla 1, el mantenimiento de estos equipos está garantizado hasta su EOL a través del contrato con número de expediente “EJIE-053-2022”.
- Se asume que, en función de cuál sea la solución propuesta por el adjudicatario a través del presente pliego, estos Firewall centrales (1500D) puedan dejar de estar integrados dentro de la gestión y reporting centralizado.
- Todos los equipos que se detallarán a continuación y cuya renovación tecnológica será objeto de este pliego tendrán su mantenimiento cubierto durante la fase de migración tecnológica a través del mantenimiento con número de expediente “EJIE-053-2022”, tal y como se ve en la tabla 1.
- Toda la plataforma de gestión y reporting será objeto de una renovación tecnológica (hardware y software) a través del presente pliego. Esto afecta a los actuales FortiAnalyzer y FortiManager.
- Todos los equipos de los centros cuyo EOL ya está publicado (modelos 100D, 200D y 200E) serán objeto de una renovación tecnológica (hardware y software) a través del presente pliego.
- Todos los equipos de los centros cuyo EOL no está publicado (modelos 101F y 60F) no serán, en un principio, objeto de la renovación tecnológica alcance del presente contrato. No obstante, en caso de que la solución tecnológica de gestión y reporting centralizado propuesta por el adjudicatario difiera de la actualmente implementada, este último deberá garantizar la correcta integración de los equipos anteriormente citados (101F y 60F) en la nueva solución, en las mismas condiciones y funcionalidades actuales, mediante su renovación tecnológica dentro del alcance del presente pliego. Esta casuística se encuentra recogida en el apartado 16, modificaciones previstas del Pliego de Condiciones Particulares.

A modo de referencia, la siguiente imagen define el marco temporal asociado a los diferentes contratos asociados al mantenimiento y renovación del equipamiento de seguridad en los centro educativos.



(*) Los equipos 1500D están bajo soporte a través del expediente EJIE-053-2022 hasta su fecha fin de vida el 31/12/2026.

(**) Los equipos actuales están bajo soporte a través del expediente EJIE-053-2022 hasta su sustitución dentro del presente contrato.

Ilustración 1: Marco temporal de los contratos asociados al equipamiento de seguridad en Centros Educativos



3 Objeto del contrato

El objeto del presente Pliego de Condiciones Técnicas es el suministro para la renovación tecnológica de la actual solución de seguridad en Red PREMIA, que engloba los servicios de seguridad y control de navegación en los centros pertenecientes al Departamento de Educación, así como la prestación de servicios de migración y soporte, con el objetivo de asegurar el servicio a los centros educativos bajo unas condiciones de operación adecuadas y en coherencia con el estado del arte actual de los sistemas de seguridad, de acuerdo con los requerimientos establecidos en el presente pliego.

La renovación tecnológica incluye el suministro, instalación, configuración, pruebas, puesta en operación, soporte y mantenimiento de la solución en todos los centros educativos pertenecientes a la Red PREMIA.



4 Ámbito geográfico

El ámbito de aplicación del presente contrato se corresponde con los setecientos sesenta y cuatro (764) centros educativos repartidos por la Comunidad Autónoma Vasca (CAV), que cuentan actualmente con equipamiento (hardware y software) perteneciente a la infraestructura de seguridad y control de navegación del Departamento de Educación, así como los edificios de EJIE en Avda. Mediterráneo 14, y Gobierno Vasco en Lakua, en calle Donostia-San Sebastián 1 (ambos en Vitoria-Gasteiz), donde se localizan los CPDs.

En el “Anexo I PCT_Centros Educativos Red PREMIA” del presente pliego se recoge el listado detallado de los centros educativos pertenecientes a la Red PREMIA, su localización geográfica, clasificación, etc.

En caso de errores, omisiones o modificaciones en la distribución geográfica de los equipos objeto de renovación, el adjudicatario deberá asumir los servicios necesarios que cubran dichos cambios sin que suponga un coste adicional para EJIE.

Para ello, el adjudicatario realizará de forma previa y, al inicio del contrato, una revisión del inventario de los equipos objeto de renovación a fin de contrastar los datos que figuran en el Anexo I con la situación real.



5 Alcance del contrato

5.1 Suministro de equipamiento

El adjudicatario deberá suministrar el equipamiento hardware y software, así como las licencias asociadas y soporte del fabricante, que seas necesarios para la renovación de la actual solución de Seguridad, que dota a los centros educativos de la Red PREMIA de servicios de seguridad LAN, servicios de control y navegación segura a Internet y servicios DHCP, de acuerdo con los requerimientos técnicos establecidos en el capítulo 6 del presente pliego.

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.

El presente contrato incluye el suministro y renovación del conjunto de software y licencias necesarias para la prestación de requerimientos y servicios solicitados hasta el 31 de diciembre de 2023.

El licenciamiento será en cualquier caso el necesario para soportar el número de usuarios de la Red PREMIA durante el periodo de vigencia del contrato, independientemente del volumen de usuarios que implique, y para las funcionalidades solicitadas, incluyendo las actualizaciones del software de las diferentes soluciones, así como las suscripciones a servicios que requieran actualizaciones continuas como son antivirus, categorías de navegación, etc.

El adjudicatario deberá implementar la misma solución en cada uno de los centros educativos indicados a fin de disponer de un sistema uniforme y homogéneo.

El adjudicatario desplegará la solución en los CPDs de la red (ubicados en los edificios de EJIE y LAKUA) y en los centros educativos.

La solución deberá incluir, además de los equipos de protección perimetral de la red (firewall) de los centros actualmente integrados en la Red PREMIA:

- Una plataforma de gestión que posibilite la administración remota y centralizada de la totalidad de los firewalls con su garantía, licencias y soporte del fabricante. Esta plataforma podría ser virtual, albergándose en el Tenant de Hezkuntza dentro de BATERA, proporcionando EJIE la infraestructura de virtualización necesaria.
- Una plataforma de centralización de logs y reporting que cumpla los requisitos de disponibilidad y capacidad especificados en el capítulo 6 del presente pliego. Esta plataforma **NO puede ser albergada en el Tenant de Hezkuntza** dentro de BATERA por sus requerimientos de consumo de almacenamiento.

Las plataformas de gestión y reporting tendrán dedicación exclusiva a este proyecto, no pudiendo reutilizarse ninguna plataforma existente actualmente en el ámbito de EJIE/BATERA/HEZKUNTZA.

En general quedan incluidos en el alcance del contrato el suministro e instalación de todos los equipos especificados 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, conexión, 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.



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.

5.2 Instalación, configuración, migración y puesta en marcha

El adjudicatario dentro del alcance del presente contrato deberá acometer los trabajos de instalación, configuración, migración, pruebas y puesta en operación de la solución propuesta, incluyendo:

- Descripción detallada del diseño y arquitectura de la solución propuesta para su validación por EJIE.
 - Descripción detallada del plan de migración a seguir para garantizar la continuidad del servicio y convivencia de la nueva solución con la existente para su validación por EJIE.
 - Plan de trabajo que garantice los plazos establecidos y que deberá ser validado por EJIE.
 - Traslado e Instalación de equipamiento en centros educativos y CPDs (EJIE y LAKUA) en coherencia con la arquitectura de solución propuesta y validada previamente por EJIE.
 - Colaboración con EJIE en la definición y actualización del catálogo de servicios que pueda ofrecerse a las entidades que hagan uso del servicio objeto del presente expediente (modelado del servicio).
 - Configuración de la solución y puesta en marcha del conjunto de tecnologías propuestas, y migración de servicios, incluyendo:
 - ✓ Configuración de equipos, definición de plantillas, despliegue de políticas de seguridad y, en general, todas aquellas tareas necesarias que aseguren la correcta migración de la solución actual. Todo ello sin impacto en funcionalidad, manteniendo, al menos, las funcionalidades, configuraciones y políticas equivalentes a las actuales, y con impacto mínimo en el servicio, asumiéndose un impacto mínimo en los propios procesos de migración.
- Esto aplica tanto a elementos de seguridad ubicados en los centros (Firewall centros) como al entorno de gestión y reporting centralizado.
- ✓ Plan de Pruebas y su ejecución, para asegurar la adecuada puesta en marcha de los servicios.
 - ✓ Transferencia de conocimiento a EJIE (Comunicaciones y Seguridad) sobre las soluciones y tecnologías desplegadas.
 - ✓ Documentación funcional y técnica de la solución finalmente implementada.
 - ✓ Documentación sobre el inventario final de equipamiento.

El equipamiento a suministrar por el adjudicatario deberá quedar correctamente colocado tanto en los racks de los centros como en los CPDs. Para ello, el adjudicatario deberá poner a disposición del contrato bandejas, kits de sujeción, y cualquier otro elemento necesario que garantice la correcta colocación del equipo en los armarios disponibles en cada ubicación.

El adjudicatario deberá tener en cuenta que la solución en su inicio deberá quedar funcionando con al menos las mismas políticas de seguridad y control de navegación a Internet desplegadas que la solución



actualmente operativa en Red PREMIA. Posteriormente, la solución se irá actualizando y adecuando a los requerimientos del entorno educativo a través de los servicios de Soporte.

5.3 Borrado de configuración y retirada de los equipos actuales

El adjudicatario será responsable del borrado de la configuración y la retirada de los equipos que componen la actual solución de seguridad, tanto los ubicados en las oficinas de EJIE y LAKUA como los de los centros de educación, incluyendo la retirada de elementos de montaje, alimentadores, cableado, etc. y en general cualquier elemento activo vinculado al mismo que quede en desuso con la puesta en marcha de la nueva solución. Asimismo, el adjudicatario se hará responsable de su almacenaje en condiciones adecuadas hasta su posterior retirada a punto limpio o a donde EJIE determine, respetando la normativa medioambiental correspondiente y aquellos requisitos que establezca EJIE a tal efecto.

Los equipos y elementos retirados deberán gestionarse a través de los sistemas de recogida selectiva establecidos por los productores (sistemas individuales o sistemas integrados de gestión). Al finalizar las actuaciones pertinentes, el adjudicatario deberá presentar los certificados de gestión de RAEE que correspondan a todos los equipos eléctricos y electrónicos retirados.

Finalmente se hará entrega de un Acta de retirada de material, para dejar constancia de los elementos retirados que deberá ser firmada por el adjudicatario y por EJIE.

El adjudicatario deberá garantizar en todo momento el cumplimiento de las obligaciones relativas a la LOPD recogidas Subanexo "Tratamiento de Datos Personales".

5.4 Seguimiento y control del proyecto

El adjudicatario deberá realizar un seguimiento continuo de la evolución de los trabajos alcance del presente contrato, informar en todo momento a EJIE del estado de los mismos y garantizar la actualización de la información y documentación en la plataforma designada por EJIE.

Para ello, el adjudicatario deberá elaborar los procedimientos y metodologías necesarias a fin de garantizar un correcto seguimiento y control del avance de los trabajos, así como un control documental.

El detalle de las tareas principales a realizar por el adjudicatario se encuentra recogido en el apartado 7.9 Seguimiento y control del proyecto.

5.5 Operación y explotación

Durante el despliegue y puesta en marcha de la solución, el adjudicatario deberá proveer el soporte adecuado para la operación y explotación de los servicios en los centros que se vayan migrando sobre las nuevas plataformas y tecnologías hasta su recepción provisional por parte de EJIE.

5.6 Garantía, soporte y mantenimiento

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 de como mínimo un (1) año de duración que deberá activarse a partir del 01/01/2023. Se considera recomendable que la licencia sea activada en el momento de instalación del equipamiento.
- Se incluye el software y licencias necesario para garantizar las diferentes funcionalidades y tecnologías propuestas, incluyendo su mantenimiento.
- 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, durante este periodo, EJE tendrá la posibilidad de realizar la apertura de casos y gestiones de RMAs 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).

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, EJE 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 EJE no existiendo accesos remotos permanentes.

A continuación, se indica el alcance de los servicios de mantenimiento alcance del presente contrato:

- Servicio de mantenimiento preventivo. A partir de inspecciones y/o mediciones periódicas (como mínimo 2 anuales) se realizarán propuestas orientadas a mejorar el rendimiento y/o disponibilidad de la red. Se incluye la propuesta de la línea base de monitorización para una detección temprana de problemas, el análisis de las versiones software y estado de los equipos a fin de reducir el número de incidencias a futuro en la red, la revisión hardware obsolescencia tecnológica y fechas de fin de vida, y el health check de la infraestructura para revisar la salud y configuraciones.
- Servicio de mantenimiento correctivo para la resolución de incidencias (in situ o en remoto) generadas por problemas o mal funcionamiento de los equipos incluidos en el alcance del 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 equipos.
 - ✓ Reparación y/o sustitución de elementos averiados.
 - ✓ Instalación/desinstalación de equipos, 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 fabricantes.
 - ✓ 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 EJE.
- Elaboración de informes mensuales de servicio y estadísticas de incidencias. Se realizarán informes mensuales que reflejen el detalle de los servicios prestados en ese periodo, indicándose al menos datos relativos a incidencias ocurridas, causa de las incidencias, tiempos de respuesta, tiempos de resolución, tareas y/o peticiones cursadas como pueden ser la configuración y optimización de los sistemas, revisión de las vulnerabilidades publicadas en ese periodo... con identificación del cumplimiento o incumplimiento de los niveles de servicio comprometidos. Asimismo, si se considera oportuno, se podrán poner a disposición de EJE herramientas que faciliten el seguimiento de las incidencias y la monitorización de los niveles de servicio vía Web.
 - Renovación de las garantías de equipos y de la suscripción de las licencias. Se renovarán las garantías de los equipos y la suscripción de las licencias objeto de contrato hasta el periodo de validez del contrato indicado. Todas las renovaciones y mantenimientos deberán ser oficiales y estar garantizadas por los respectivos fabricantes. La renovación del mantenimiento de los equipos objeto del contrato deberá contemplar la contratación de licencias y soportes con las mismas condiciones que tienen los equipos en la actualidad, es decir, con el mismo nivel de bundle y soporte.
 - Asunción de evoluciones sobre la misma plataforma. Aunque es un servicio ya constituido y no se prevén variaciones significativas, 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 EJE en un horario convenido y que menos afecte al funcionamiento de dichos servicios.
 - Estadísticas de uso de la plataforma. EJE podrá solicitar al adjudicatario la elaboración de un informe con toda la información relativa al servicio que la plataforma presta. EJE validará y podrá a su vez requerir la inclusión de más información en el citado informe.
 - Servicio de soporte técnico experto, abierto a las necesidades de EJE en consultas de soporte y en el ámbito de las tecnologías especificadas y horarios de atención solicitados.

5.7 Inventario de elementos y documentación as-built



Al finalizar toda la instalación 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.
- Manual de explotación, detallando los procedimientos a seguir para la realización de los pertinentes ajuste, 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.
- Protocolos de pruebas.
- Documentación para entrega del servicio a Operación de EJE, el cual da respuesta a los siguientes conceptos (Se adjunta formato de documento a considerar en Anexo):
 - ✓ Gestión de Conocimiento: Descripción y características generales del entorno, descripción de los distintos elementos que conforman la plataforma con el rol que desempeñan, configuraciones específicas 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 EJE.
 - ✓ Gestión de Backup: Definición de los backups configurados.
 - ✓ Gestión de Eventos: Definición de la monitorización necesaria y configurada en los entornos de EJE, 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 definir las 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
 - ✓ Otros Entregables: Otra documentación que pueda complementar a la anterior.



- Aquella documentación que aplique relacionada con la definición y actualización del catálogo de servicios que pueda ofrecerse a las entidades que hagan uso del servicio objeto del presente expediente (modelado del servicio).

La documentación entregada pasará a ser propiedad de EJIE.

5.8 Stock para equipamiento en centro

De forma adicional a los equipos a desplegar en centros, el licitador deberá incluir en su oferta el suministro de equipos en stock, incluyendo licencias, ante la posibilidad de crecimiento del número de centros durante el período de vigencia del contrato o para las labores de mantenimiento alcance del contrato.

Los modelos y cantidades de equipamiento de stock a suministrar se detallan en el apartado 6.3 de este documento.

Los equipos a suministrar se almacenarán en EJIE.

6 Requisitos técnicos y funcionales

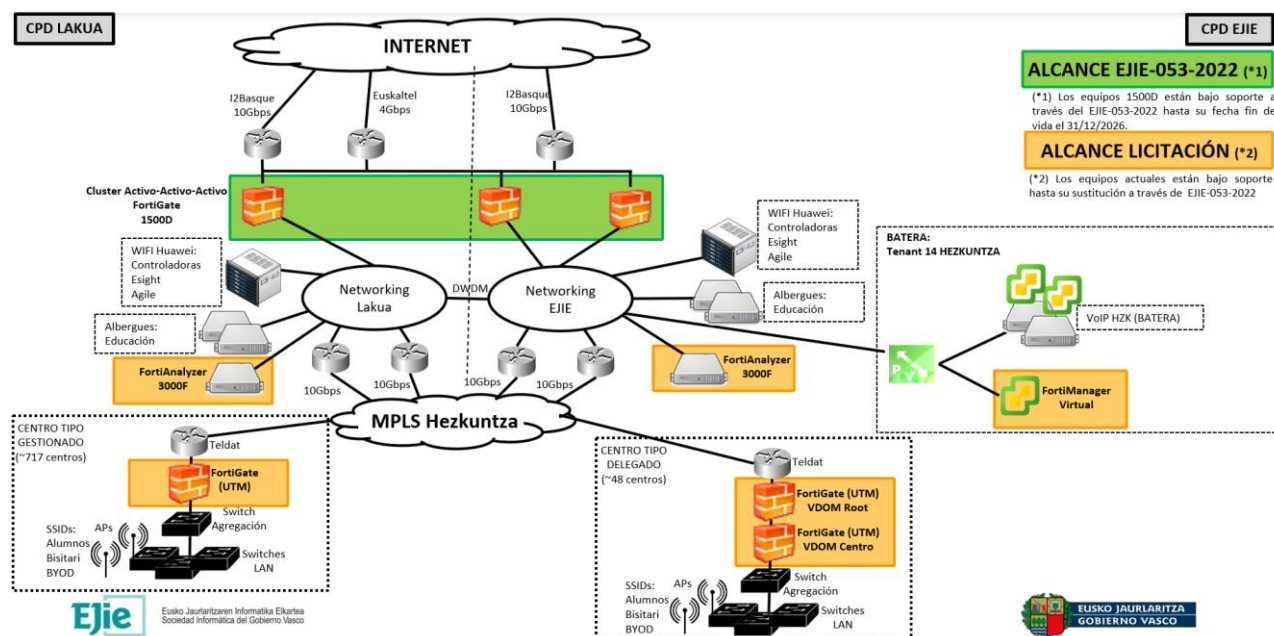
El licitador deberá tener en cuenta que el equipamiento y tecnologías a desplegar deben dar solución tanto a los servicios de seguridad LAN actuales en los centros educativos como a la solución de navegación segura a Internet de la Red PREMIA, de acuerdo con los requerimientos definidos en el presente 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 aquellos que se indican como deseables.

6.1 Arquitectura actual del sistema

Habiéndose demostrado un diseño adecuado durante los últimos años, la arquitectura general de seguridad y conectividad, en la fase inicial del proyecto, se va a mantener intacta. En la siguiente imagen se pretende reflejar, a alto nivel, la arquitectura general de la solución actual así como los elementos que son objeto de renovación tecnológica mediante el presente pliego:



Según este esquema, hay que tener en cuenta los siguientes factores:

- A nivel de conectividad, todos los centros están conectados a través de la MPLS de Red PREMIA hasta los CPDs de EJIE y LAKUA, con un agregado de 20 Gbps en cada CPD.
- A nivel de conectividad, los centros disponen de unos enlaces dimensionados según el tipo y tamaño del centro.



- A nivel de conectividad, la salida a Internet se realiza a través de los CPDs de EJIE y Lakua, contando con líneas de I2Basque y de Euskaltel para salir a Internet, disponiendo de un agregado total de 24 Gbps repartidos entre los dos CPDs.
- En los CPDs de EJIE y Lakua existe un cluster de **3 equipos FortiGate 1500D** en modo activo-activo que realizar funciones de FW y balanceo de las líneas de Internet.
- Este cluster de equipos tiene como fecha de fin de vida el 31/12/2026, por lo que, como ya se ha adelantado, **quedará fuera del alcance de este proyecto**.
- En los CPDs de EJIE y Lakua se ubican física y lógicamente los elementos que permiten centralizar la gestión y reporting de la solución actual. Esto es:
 - ✓ Servidor Virtual de Gestión ubicado en el Tenant de Hezkuntza dentro de BATERA
 - ✓ 2 Servidores FortiAnalyzer 3000F sincronizados que permiten centralizar logs y generar informes automáticamente y bajo demanda.
- Existen dos tipos de centro en cuanto a gestión del equipamiento se refiere:
 - ✓ Centros TIPO GESTIONADO: Alrededor de 716 centros. En este caso, en el centro existe un equipo adaptado a su tamaño que está gestionado por los equipos de Soporte de EJIE completamente.
 - ✓ Centros TIPO DELEGADO: Alrededor de 48 centros. En este caso, en el centro existe un equipo adaptado a su tamaño que dispone de 2 instancias virtuales (VDM) independientes. La principal es gestionada por los equipos de Soporte de EJIE. La otra instancia es gestionada por el centro, con objeto de disponer de una independencia necesaria para estos ámbitos educativos sin impactar en el VDM principal.
- A nivel de conectividad y seguridad en los centros, los equipos Fortigate locales realizan las siguientes funciones principales:
 - ✓ Networking
 - ✓ Firewall
 - ✓ Control de Navegación (Filtrado URLs, control de aplicaciones, Antimalware, Gestión SSL)
 - ✓ DHCP
 - ✓ Balanceo de líneas en diversos modos: balanceo SDWAN, rutas estáticas, policy routes.
 - ✓ IPS
- A nivel de disponibilidad en los centros, no se considera necesario disponer de cluster en cada centro. Para cubrir los escenarios de contingencia se dispondrá de STOCK para poder sustituir el equipamiento averiado en corto espacio de tiempo.

Adicionalmente, de cara a la evaluación del coste de migración, se proporcionan los siguientes datos de alto nivel en lo que a políticas y reporting se refiere:

- Nº Políticas / Reglas:
 - ✓ 60 políticas gestionadas de manera central:



- 20 por tipo de centro:
En función de si son capa 2 o 3, si el centro tiene Wifi, VoIP, ambas o ninguna, etc.
La mayoría tienen entre 20 y 30 reglas compartidas que componen la “política básica”.
Adicionalmente, cada política tiene otras 100-200 reglas que se aplican a centros específicos.
- 40 específicas de algunos centros con configuraciones especiales.
- ✓ Adicionalmente las políticas de los centros delegados.
- Nº Reports
 - ✓ Alrededor de 50 informes automatizados:
 - 40 para centros delegados, mensuales.
 - 3 informes para Departamento, mensuales.
 - Resto informes relativos a malware, eventos, etc. semanales.
 - ✓ Adicionalmente, existen plantillas para lanzar informes puntuales para centros. :
- Usuarios:
 - ✓ Los usuarios en general autentican en base a grupos de dominio, configuración que hay que regularizar además en este proyecto.
 - ✓ Existen usuarios locales en los centros delegados, que seguirán del mismo modo. Son un total de 320 usuarios aproximadamente repartidos de forma no uniforme entre los diferentes centros.

6.2 Requisitos de diseño de la solución

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

- 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.
- 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:
 - ✓ Los 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.
 - ✓ La solución debe permitir la incorporación de nuevos equipos de forma flexible, tanto en cantidad como en tipología (mismos modelos ofertados u otros diferentes), a lo largo de la vida del contrato.
- El elemento Firewall de los centros realizará, al menos, funciones de networking, seguridad y control de navegación.



- Los elementos Firewall de los centros no se requiere en principio que estén en HA, aunque deben soportar ese tipo de configuración. Ante una incidencia hardware en un centro el equipo se sustituirá por otro en stock, gestionándose un RMA.
- Los denominados CENTROS DELEGADOS deben mantener su capacidad de gestión de un equipamiento Firewall que no impacte sobre el equipamiento Firewall que los conecta con la red WAN y que es gestionado por el equipo de Soporte de EJE. La gestión de los centros debe poder ser autónoma, no impactando ni a nivel de configuración ni a nivel de rendimiento. Esto requiere que la solución permita hacer uso de tecnologías de virtualización (con control de recursos) sobre un equipamiento físico único que no podrá ocupar más de 1 U, que es el tamaño de los actuales equipos que se van a sustituir.
- Las acciones realizadas en los equipos delegados también quedarán recogidas en los sistemas centrales de gestión y reporting, aunque se puedan realizar de forma local.
- No se admitirán soluciones que impliquen instalación de agentes en puestos.

Se recuerda que el adjudicatario puede considerar que el equipamiento para la gestión centralizada sea virtual y esté albergado en BATERA (Tenant Hezkuntza), proveiendo EJE la infraestructura para albergar este equipamiento virtual. Sin embargo, el licitador debe proveer la infraestructura relacionada con el almacenamiento de logs centralizados.

6.3 Firewall Centros: Tipos, Cantidad y Rendimientos

6.3.1 Tipos y Cantidad

Aunque en el diseño de 2015 se tuvieron en cuenta tres tipos de centro, la experiencia durante estos años y las previsiones de evolución existentes, llevan a considerar óptimo establecer, en este contrato, únicamente dos (2) tipos de centro y, por lo tanto, dos (2) modelos de Firewall a proveer por parte de los licitadores.

Adicionalmente, si lo requiere para el cumplimiento de requisitos relacionados con los CENTROS DELEGADOS, el adjudicatario podrá proponer un tercer modelo diferente a los anteriores para el caso de dichos centros.

En el “Anexo I PCT_Educativos Red PREMIA” del presente pliego se incluye información del modelo deseado para cada una de las sedes alcance del presente contrato.

De cara a determinar cuántos equipos de cada modelo son necesarios y en qué centros hay que ubicarlos se tendrán en cuenta tanto el ancho de banda contratado actualmente como el hecho de ser un centro tipo delegado o no serlo. Así, a continuación se indica la cantidad de equipos de cada tipo que deberían aprovisionarse inicialmente (*1) para cubrir los actuales equipos productivos:

Modelo	Características de Centros (CAUDAL ACTUAL/TIPO DE CENTRO)	Cantidad
Modelo A	< 200 Mbps	590
Modelo B	>= 200 Mbps	81
Modelo C (*2)	CENTROS DELEGADOS	42



(*2) Idealmente, el Modelo C será el mismo que el Modelo B si éste cumple todos los requisitos relacionados con los Centros Delegados.

Adicionalmente, se provisionarán equipos **licenciados** que realizarán simultáneamente funciones de STOCK y de atención a crecimientos puntuales. Teniendo en cuenta que debe haber STOCK en las tres provincias por cuestiones de tiempos de respuesta, se deberán proporcionar los siguientes equipos adicionalmente.

Modelo	Objetivo	Cantidad
Modelo A	STOCK + Crecimiento	6
Modelo B	STOCK + Crecimiento	3
Modelo C (*3)	STOCK + Crecimiento	7

(*3) Únicamente se provisionará STOCK de este modelo cuando sea necesario utilizarlo y se realizará a través de una modificación prevista del pliego, no sería objeto de la provisión inicial. Si en los centros delegados se provisiona Modelo B porque cumple todos los requisitos, no será necesario un tercer modelo C.

Sumando ambas cantidades, el número total de equipos que debe suministrar el licitador inicialmente (*1) se refleja en la siguiente tabla:

Modelo	Cantidad
Modelo A	596 Equipos
Modelo B	84 Equipos
Modelo C	42 – 49 Equipos (*4)
TOTAL	722 - 729 Equipos (*4)

(*1) Todos los equipos de los centros cuyo EOL no está publicado (modelos 101F y 60F) no serán, en un principio, objeto de una renovación tecnológica. Sin embargo, si la solución de gestión y reporting que sea adjudicataria de este pliego no fuera capaz de integrar este equipamiento de forma nativa, parte de estos equipos también serían objeto de una renovación tecnológica a través de este pliego (modificación prevista de adquisición de 40 equipos Modelo A y 5 equipos Modelo B y 6 equipos Modelo C).

(*4) El número de equipos inicial dependerá de si el Modelo C es el mismo que el Modelo B debido al número de equipos de stock que se solicitan. En caso de ser el mismo modelo, serán 42 Modelo C y 722 equipos Totales respectivamente. En caso de ser diferentes, serán 49 y 729 equipos respectivamente. En cualquier caso, la incorporación del stock de modelo C sería a través de modificación prevista.

6.3.2 Rendimientos

A continuación se muestra una tabla en la que se representan los parámetros mínimos que debe cumplir individualmente cada uno de los equipos proporcionados, en función del modelo.

En lo referente a medidas relacionadas con volumen de tráfico y conexiones simultáneas, los datos deben corresponder a **medidas realizadas con tráfico real y con todos los módulos de protección activados**,



no siendo válidas las medidas en condiciones ideales. El licitador deberá proporcionar los rendimientos ofrecidos por cada modelo en las condiciones solicitadas.

Requisito	Modelo A	Modelo B	Modelo C
Rendimiento mínimo con todos los módulos activados.	≥ 750 Mbps	≥ 1 Gbps	≥ 1 Gbps
Nº Interfaces 1 GE RJ45 WAN-LAN	≥ 4	≥ 8	≥ 8
Nº sesiones concurrentes	≥ 200.000	≥ 300.000	≥ 300.000
Soporte de Instancias Virtuales de Firewall (para Centros Delegados)	Opcional	Opcional	Obligatorio (licenciado)

6.4 Firewall Centros: Requisitos Networking

Todos los firewall de los centros propuestos deben cumplir los siguientes requisitos obligatorios que deben estar licenciados:

- Dual Stack: IPv4 e IPv6
- VLANS: Deberá soportar 802.1Q
- LACP: Deberá soportar LACP 802.3ad para poder agregar interfaces.
- Point-to-Point Protocol over Ethernet (PPPoE).
- 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
- Balanceo de líneas de Internet: Debe implementar mecanismos para balanceo de líneas de comunicaciones. Debe permitir tanto balanceos dinámicos con reparto de carga como balanceos controlados por aplicaciones, puertos/protocolos o IPs. Así, debe permitir, al menos, los siguientes escenarios:
 - ✓ Que un centro vaya a las aplicaciones corporativas (servidores web, VoIP, etc.) por la MPLS, mientras sale a Internet por una o varias (en reparto de carga) líneas dedicadas a navegación.
 - ✓ Que un centro salga habitualmente a Internet por una línea (o varias en reparto de carga) y, en caso de error de esa línea (o de todas ellas si son varias), pase a ir por la MPLS.



- ✓ Que un centro saque a Internet a ciertas LANs del centro por la MPLS y a otras por una o varias (en reparto de carga) líneas de Internet, rutando además a todas las LANs por las mismas líneas en caso de fallo de las que usan habitualmente.
- DHCP: Deberá ser capaz de actuar como servidor DHCP en todos sus interfaces de red. También debe soportar DHCP Relay.

La solución deberá realizar el registro de asignaciones/liberaciones de las direcciones IP.

- 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.

6.5 Firewall Centros: Requisitos Seguridad, VPN, Autenticación y Delegación.

Todos los firewall de los centros propuestos deben cumplir los siguientes requisitos obligatorios que deben estar licenciados:

- 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).
- 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.
- 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. Como mínimo, debe permitir establecer un role que ofrezca lectura de logs y configuración y escritura en la configuración de interfaces de red y DHCP.
- VPN: Soporte, como mínimo, para dos tipos de VPN
 - ✓ Usuario final con cliente pesado: Deberá permitir la asignación de IPs y DNS controlados desde el FW.
 - ✓ Site2Site

El equipamiento deberá cumplir los estándares de mercado:

- ✓ IPSec VPN (IPv4 e IPv6) (con soporte de NAT)



- ✓ PPTP
- ✓ L2TP

6.6 Firewall Centros: Requisitos Control de Navegación a Internet

Todos los firewall de los centros propuestos deben cumplir los siguientes requisitos obligatorios que deben estar licenciados:

- Filtrado Web/URL, en base a múltiples categorías de navegación y con las siguientes características adicionales:
 - ✓ Capacidad multilingüe de la plataforma. Base de datos de URLs multilingüe y Análisis inteligente y multilingüe de los contenidos en tiempo real
 - ✓ La solución debe disponer de una cantidad de categorías de URL que permitan un acceso granular a los recursos de Internet. Mínimo 40 categorías diferentes.
 - ✓ Deberá contar con categorías de seguridad específicas.
 - ✓ Permitirá crear categorías propias
 - ✓ Permitirá que una URL pueda pertenecer a varias categorías simultáneamente
 - ✓ Clasificación de los contenidos en tiempo real.
 - ✓ El sistema incluirá la actualización permanente de la base de datos de URLs y categorías para todo el periodo de vigencia del contrato.
 - ✓ Incorporación automática de actualizaciones. La solución debe ser capaz de recategorizar en tiempo real el contenido de cualquiera de las categorías existentes.
 - ✓ Se deberá garantizar la correcta diferenciación de las categorías educativas que contienen algún contenido susceptible de ser bloqueado en otras categorías. Por ejemplo: "Educación sexual".
 - ✓ Posibilidad de gestionar listas blancas/listas negras.
- Control de protocolos y aplicaciones: Capacidad para identificar aplicaciones y generar reglas en base a ellas.
 - ✓ Un mínimo de 1000 aplicaciones, incluyendo aplicaciones Web 2.0, e incluyendo las aplicaciones típicas de ámbitos educativos.
 - ✓ Las aplicaciones se deberán detectar en todos los puertos, no sólo en los puertos estándar.
 - ✓ La solución agrupará las aplicaciones en categorías, de forma que se puedan crear reglas por esas categorías.
- Posibilidad de aplicar políticas de filtrado de URL y control de aplicaciones diferentes en función de diferentes consideraciones (IPs, usuarios/grupos, etc.)
- Posibilidad de personalizar la página de bloqueo, permitiendo mostrar una página de bloqueo en euskera y castellano con variables asociadas a la página bloqueada.
- Antivirus de navegación Web/Antimalware/Antispyware (antivirus perimetral para tráfico web, análisis de reputación web, análisis de comportamiento e identificación de actividades sospechosas, análisis en tiempo real de amenazas tipo troyanos, malware, phishing, protección contra botnets, antispam,...).



Se debe incluir la **actualización continua** durante el periodo de vigencia del contrato a las bases de datos de virus, malware,..

- Inspección selectiva de tráfico SSL/https, con “rotura de túnel”.

6.7 Requisitos Gestión, Logs y Reporting centralizado

Se requiere de una solución de administración, gestión y control de navegación que sea centralizada y que soporte diferentes perfiles de administración.

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. Adicionalmente, los equipos de los centros deben poder ser gestionados de forma autónoma y local si así se requiere en un momento dado o si se prefiere gestionar de ese modo en algún caso.

Aunque inicialmente habrá que migrar las políticas existentes actualmente, el objetivo del Departamento es disponer de una serie de políticas generales en función de los diferentes tipos de centro y, sobre ellas, realizar cambios autorizados por el Departamento.

A través de la solución de administración se realizarán las siguientes labores:

- Administración y configuración centralizada de los equipos y solución (estado de equipos, despliegue de políticas, definición de nuevas políticas,...).
- La solución debe permitir la administración local de los equipos en caso de necesidad o preferencia (Los Centros Delegados actualmente trabajan en este modo habitualmente en el FW gestionado por el centro), de forma que la gestión centralizada únicamente respalde configuraciones y, en todo caso, centralice logs y reporting.
- 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 de cambios, configuraciones, accesos,...y las estadísticas de navegación **durante un período de al menos 2 años**. Como se ha comentado previamente, 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.
- 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.
- 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, a nivel de usuario y de forma agregada (conjunto de la red).
- La solución debe registrar los cambios realizados respecto a las políticas globales definidas por el Departamento. Asimismo, debe ofrecer la posibilidad de recuperación de las políticas de inicio 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.
- 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 por grupos de los mismos y también en su totalidad agregada.
- Se mencionan algunos datos de interés en los informes:
 - ✓ Estadísticas de tráfico:
 - Ancho de banda consumido, sesiones,...
 - Usuarios por ancho de banda consumido, usuarios por sesiones, usuarios activos por periodo de tiempo,...
 - Top destinos por ancho de banda y sesiones
 - Aplicaciones más utilizadas por ancho de banda consumido
 - Top de usuarios con más consumo de ancho de banda
 - ✓ Sitios web más visitados (permitidos)
 - Por usuario
 - Por tiempo de navegación
 - Por ancho de banda consumido
 - Sitios y aplicaciones top permitidos
 - ✓ Categorías visitadas por tiempo de navegación, sitios web más visitados de forma recurrente, categorías por consumo de ancho de banda,...
 - ✓ Aplicaciones por categoría, aplicaciones de riesgo elevado por categoría,...
 - ✓ Intentos de accesos a páginas bloqueadas, usuarios con bloqueos de navegación reincidentes, categorías/sitios web bloqueados usualmente,...
 - ✓ Intrusiones detectadas:
 - Malware detectado, víctimas del malware,...
 - Redes Botnet detectadas, víctimas de redes botnet,...
 - Orígenes de las intrusiones,...
 - Intrusiones por tipo, severidad, tiempo, intrusiones bloqueadas,...
 - ✓ Ataques sobre servicios https
 - ✓ Top de usuarios, dispositivos, con reputación dudosa
 - ✓ Otros

6.8 Otros requisitos técnicos y funcionales



- Monitorización de dispositivos móviles: Posibilidad de monitorización de dispositivos móviles en centros, desde las soluciones y herramientas de gestión centrales propuestas por el adjudicatario, de forma que sea posible identificar sistemas operativos, tipos de dispositivos, mostrar información de uso, etc.
- Certificaciones de Seguridad: Como mínimo deberá cumplir la siguiente certificación de seguridad:
 - ✓ CCN-CERT: Ante la posible aparición de servicios del ámbito de Educación de categoría ALTA en el ámbito del Esquema Nacional de Seguridad, EJE 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 inferiores o anteriores del producto (versiones publicadas hace menos de 2 años).

6.9 Checklist de requerimientos

Como documentación anexa a la propuesta técnica, el licitador deberá adjuntar el checklist de requerimientos solicitado a través del presente expediente, que recoja los requisitos de obligado cumplimiento.

Requisito		Cumple (Sí/No)	Descripción
-----	-----		Nº pág oferta en la que se describe el requerimiento



7 Servicios Profesionales

7.1 Servicios de consultoría y diseño de la solución

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

- La relación de datos de partida disponibles sobre el equipamiento alcance de la renovación.
- Las características de la solución actual implementada en los centros: arquitectura del sistema actual, funcionalidades, configuraciones, etc.
- Los requisitos preliminares y características mínimas solicitadas sobre la nueva solución: gestión centralizada, logs, reporting, etc.

Conocida la situación de partida y objetivos preliminares para la implementación de la nueva 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 de del sistema de seguridad.
- Revisión/adecuación de criterios y requisitos de cobertura, seguridad, control de navegación, 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 EJE.

7.2 Plan de migración para la convivencia de servicios

El adjudicatario deberá elaborar un plan de migración para garantizar la continuidad del servicio y la convivencia de la nueva infraestructura con la existente hasta su completa migración, garantizando que el impacto a los centros educativos 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) cuando convivan dos sistemas en paralelo.
- Se deberá plantear si procede, planes de migración diferenciados atendiendo a diferentes casuísticas que se puedan encontrar.
- El plan deberá identificar las diferentes fases en las que acometer el proceso de cambio, 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 migración adoptada.
- Por otro lado, dependiendo de la situación actual y modelo de centro podrán considerarse planes y estrategias diferentes.
- El adjudicatario deberá tener en cuenta estos horarios en los que se podrá actuar en centros educativos para minimizar el impacto de las actuaciones: de lunes a viernes laborables por las tardes (a partir de las 15:00 previsiblemente).
- La migración de todos los centros se deberá abordar **antes del 30/09/2023**. Dentro de este plazo, hay fechas límite de migración específicas para ciertos centros dependiendo del modelo de equipo



instalado en la actualidad que están relacionadas con la fecha de fin de vida del equipamiento que se describe en el apartado 2 del presente pliego (ver detalle de plazos límites en tabla inferior)

- EJE seleccionará ciertos centros de educación piloto cuya migración deberá efectuarse antes de comenzar el despliegue masivo. La migración 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)

En la siguiente tabla se indican las fechas límite para acometer la migración de los centros en base al modelo de equipo instalado.

Modelo de equipo	Número de centros	Fecha límite de migración para centros con el modelo de equipo indicado
FortiGate-200D	87	22/05/2023
FortiGate-100D	624	26/07/2023
FortiGate-200E	2	30/09/2023
FortiGate-60F	25 (*)	30/09/2023
FortiGate-101F	26 (*)	30/09/2023

(*) La migración de estos centros solo procede si se aplica la modificación prevista de este contrato relativa a la adquisición de equipos para instalar en centros que tengan en la actualidad los modelos FortiGate-60F y FortiGate-101F

Respecto a la migración de las plataformas de gestión, logs y reporting, deberá efectuarse de tal forma que estén operativas antes de la migración del primer equipo (el primer equipo será el correspondiente a uno de los centros seleccionados como piloto)

7.3 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 en EJE y Lakua y conectividad requerida para configuración de la arquitectura propuesta.

El adjudicatario deberá considerar las directrices que se establezcan en los centros y Departamento 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 parchado en los racks de los centros de la Red PREMIA.

- Definición de plantillas de configuración de equipos para la puesta en marcha de las soluciones y servicios a migrar, incluyendo las plataformas de administración y reporting, así como la



elaboración de plantillas para aplicación de políticas de seguridad y navegación establecidas por el Departamento y políticas de seguridad LAN a nivel de centro

- 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 y los servicios migrados, de acuerdo a los requerimientos establecidos en el presente pliego.
- Establecimiento de unos primeros centros de educación como centro 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 migración (Plan de Migración) en la convivencia de infraestructura vieja y nueva y garantizar la continuidad del servicio en estos casos.
 - ✓ 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 Migración 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 centros**.

Las propuestas de centros piloto se definirán conjuntamente con EJIE.

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

7.4 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/migración 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 educativos.
- Elaboración conjunta de procedimientos y metodologías orientados al seguimiento y control de avance del despliegue, y control documental.
- Revisión de las plantillas para el conjunto de documentación del proyecto a elaborar, a partir de los datos de partida facilitados por EJIE. En caso de ausencia de plantillas, definición de propuestas de documentación, para posterior validación por EJIE.

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

7.5 Mantenimiento del equipamiento

7.5.1 Mantenimiento correctivo. 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.
- 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 del usuario final.
 - ✓ Leves: incidencias que no impiden el funcionamiento del servicio, pero que degradan su uso de manera leve, sin suponer incidencias de usuario 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.

7.5.2 Mantenimiento preventivo. Acuerdos de nivel de servicio

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

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 de los equipos buscando el reducir el número de incidencias a futuro en la red.
- Revisión hardware 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 migración.
- Inconvenientes de la no migración.
- Estimación de esfuerzo e impacto sobre el servicio.



- Observaciones si las hubiera.

7.5.3 Stock de equipos

El adjudicatario podrá disponer del equipamiento de stock que considere necesario para asegurar los niveles de servicio comprometidos.

7.5.4 Medios técnicos y herramientas de apoyo al servicio

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

El adjudicatario deberá disponer de las herramientas adecuadas y necesarias para el registro de las incidencias y peticiones solicitadas en relación con el servicio, documentación de actuaciones para su resolución y medición de los niveles de servicio solicitados.

Asimismo, el adjudicatario deberá 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.

7.6 Transferencia de conocimientos a EJIE

Como criterio general, durante la ejecución de los trabajos objeto de la contratación, el adjudicatario se compromete a facilitar en todo momento a EJIE 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 así como a los CENTROS DELEGADOS, que cuentan capacidad para la gestión autónoma de los equipos Firewall que tienen instalados. Las sesiones de transferencia de conocimiento comprenderán, al menos, los siguientes contenidos:

- Introducción al servicio de protección perimetral de red (Firewalls)
- 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 que pertenecen a la Red Premia.
- Gestión y operación del servicio: monitorización, configuración del servicio, diagnóstico de averías, datos de uso del servicio, utilización plataformas centrales... Se mantendrá de forma expresa una sesión sobre la monitorización.

La transferencia de conocimiento deberá garantizar que el equipo de soporte de EJIE 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.

En el caso de los CENTROS DELEGADOS, el adjudicatario deberá asegurar que adquieren el conocimiento necesario sobre la nueva solución que les permita operar y gestionar de forma autónoma los equipos que se instalen en los mismos.



Las sesiones de tranferencia de conocimiento deberan ser impartidas, en la modalidad que EJIE/CENTROS DELEGADOS 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:

- Sesiones EJIE: veinte (20) horas, distribuidas en las sesiones que EJIE estime necesarias para adaptarse a la disponibilidad del personal de EJIE
- Sesiones CENTROS DELEGADOS: doce (12) horas, distribuidas en tres (3) sesiones según disponibilidad del personal designado por los CENTROS DELEGADOS.

Independientemente de estas sesiones, se incluirá la prestación de servicios de transferencia de información a todos los centros educativos definidos en el presente pliego, para la operación a través de las plataformas de gestión delegada. La organización de estos servicios dependerá de la necesidad y demanda de los centros que surja durante el período de vigencia del contrato.

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.

7.7 Garantía, soporte y mantenimiento de la solución.

7.7.1 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.

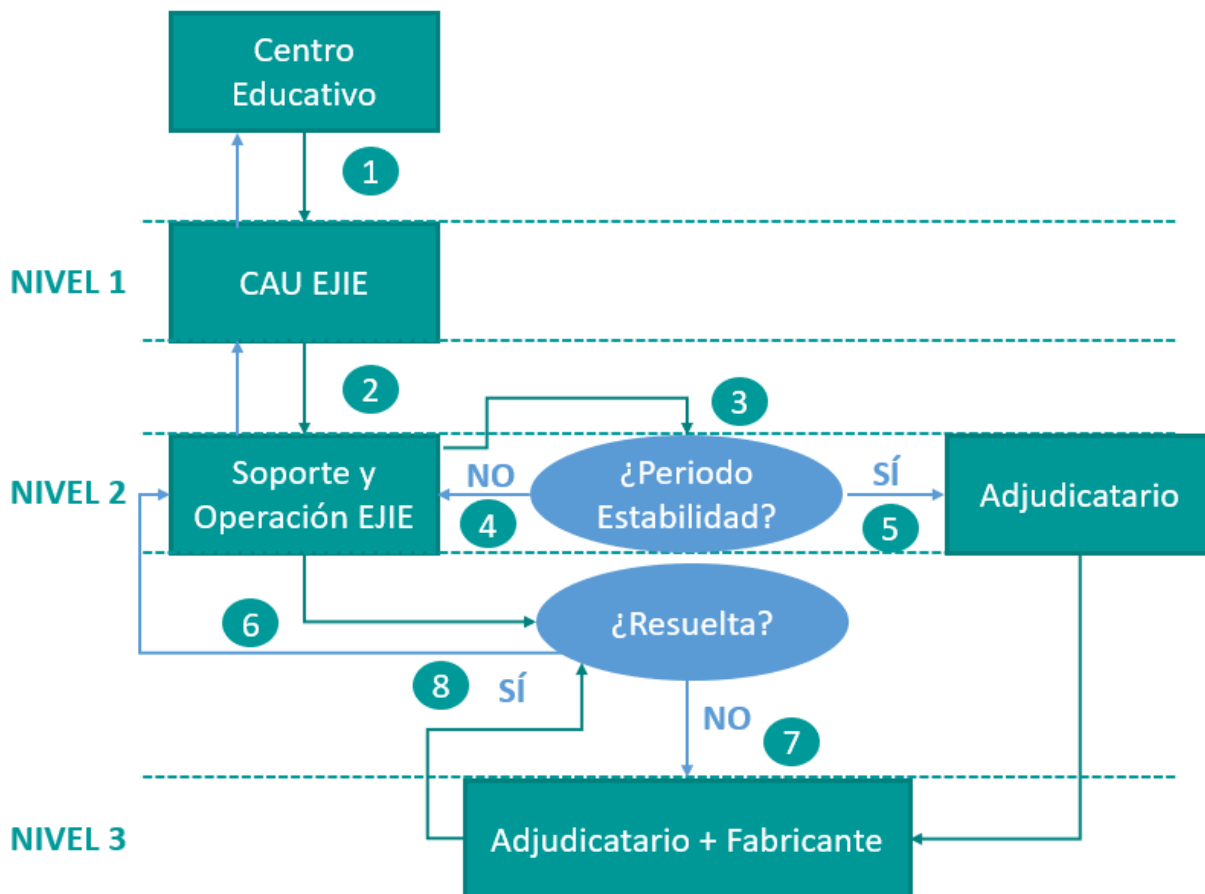
El plazo de garantía de los suministros e instalaciones no podrá ser inferior **al 31 de diciembre de 2023**.

Así mismo, 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 (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.

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 siguiente esquema muestra el flujo a seguir para la gestión de las incidencias del servicio:



- 1 El Centro Educativo envía la incidencia al CAU de EJIE
- 2 El CAU remite la incidencia al NIVEL 2 de EJIE
- 3 El NIVEL 2 comprueba si el sistema se encuentra dentro del periodo de estabilidad en el que la gestión es realizada por el adjudicatario
- 4 Si se ha superado el periodo de estabilidad del sistema, la gestión de la incidencia pasa a ser responsabilidad del NIVEL 2
- 5 Si no se ha superado el periodo de estabilidad del sistema, la gestión de la incidencia pasa a ser responsabilidad del adjudicatario
- 6 El NIVEL 2 resuelve la incidencia y se lo comunica al CAU quién a su vez se lo comunica al Centro Educativo
- 7 Si la incidencia no ha podido ser resuelta por el NIVEL 2, éste se la envía al NIVEL 3 para su gestión
- 8 El NIVEL 3 resuelve la incidencia y se lo comunica al NIVEL 2 quién a su vez se lo comunica al CAU y éste al Centro Educativo

7.7.2 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 HW o SW 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 cambio, se aplicarán las penalizaciones definidas en el capítulo correspondiente del presente documento.

7.8 Recepción provisional de las instalaciones en centros

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

- Validación por parte de EJIE de la instalación realizada.
- Verificación por parte de EJIE del correcto funcionamiento del servicio.
- Entrega y validación por parte de EJIE de la documentación as-built asociada a cada uno de los centros.

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 cuarenta y ocho (48) horas, tras la realización de la instalación y validación del funcionamiento del servicio en las condiciones requeridas en el presente pliego.

7.9 Seguimiento y control del proyecto

7.9.1 Coordinación global del proyecto

EJIE será responsable de la gestión global del proyecto y desarrollará, entre otros, los siguientes trabajos principales:

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

7.9.2 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 mecanismos 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 migración de los servicios se realice con éxito y mínimo impacto posible:

- Centros educativos y Departamento,
- CAU de Educación, quien supervisa el día a día de la operativa en centros,
- EJIE como operador de la solución de navegación segura a Internet actual,
- Proveedores de líneas de comunicaciones.

El adjudicatario designará un Jefe de Proyecto como interlocutor principal con EJIE para el control de ejecución del proyecto.

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

- Realizará un 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 con aquellas a desarrollar por parte de EJIE (validación de diseños, validación replanteos y planes de trabajo, pruebas, etc.).
- Dispondrá en todo momento de los medios necesarios para garantizar el cumplimiento del plan, y definirá metodologías para control de riesgos y definición de propuestas de mitigación de los mismos.
- Igualmente dispondrá en todo momento de los medios adecuados que garanticen los resultados esperados, en calidad y servicio final.
- Asistirá junto con los técnicos que se estime conveniente a las reuniones de seguimiento y revisiones técnicas que convoque EJIE y con la periodicidad que ésta 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.).
- Organizará el conjunto de recursos necesarios para la ejecución de los trabajos de instalación y del equipo de backup siempre con el objetivo de cumplir la planificación definida.

7.9.3 Gestión documental



Para el seguimiento del proyecto, EJE 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 EJE sobre los avances de proyecto, y herramienta de intercambio para la validación de la documentación de proyecto.

El adjudicatario será el responsable del registro y volcado de la documentación señalada:

- Datos de partida (listados de centros, equipos, etc.).
- Documentos sobre el diseño de la solución y plan de migración.
- Criterios y acuerdos relativos a la ejecución de los trabajos e instalaciones en centros.
- Planificación del proyecto:
 - ✓ Planificación acordada (cerrada) de actuaciones particulares en centros educativo (instalaciones, pruebas, etc.).
 - ✓ Informe completo de los avances diarios de despliegue de cada centro educativo, relativo a los eventos sucedidos en el día laborable anterior (revisión diaria).
- Proyectos finales incluyendo los resultados de las instalaciones realizadas y las pruebas en centros educativos.
- Documentación de inventario y actas de retirada y entrega de material/servicio en centros educativos
- 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.

7.9.4 Reuniones de seguimiento

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

7.10 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 EJE. 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 EJE. 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. EJE 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 EJE, 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 educativos alcance del contrato. 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 migración.

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:



- **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.
- **Equipo de despliegue:**
 - Un ***Coordinador de los recursos de despliegue***, necesario como consecuencia del elevado número de recursos de instalación a destinar al proyecto.
 - **7 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 Premia (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.
- **Equipo para la prestación de los servicios de mantenimiento**, 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



8 Anexos

8.1 Anexo I PCT_Centros Educativos Red Premia

En este anexo se aporta información relativa a las sedes objeto de este proyecto: ubicaciones, equipos actuales y modelos de equipo requeridos.

8.2 Anexo II PCT_Checklist requisitos técnicos

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

8.3 Anexo III PCT_Índice diseño de la solución

Este anexo incluye el índice a seguir por el adjudicatario para la elaboración del documento de diseño de solución que entregará al finalizar el proceso de construcción y migración en las condiciones que se explican en este PCT.

8.4 Anexo IV PCT_Plantilla CMDB

Este anexo es una plantilla que deberá ir completando el adjudicatario durante el proceso de construcción y migración de la solución en las condiciones que se explican en este PCT de tal forma que, a la finalización de dicho proceso, contenga el inventario completo de la solución.