PLIEGO DE PRESCRIPCIONES TÉCNICAS DE LA ACTUACIÓN A5.1.3 Y DE LA ACTUACIÓN A5.2.1 PARA EL REPLANTEO Y MEJORA DE LA RED DE COMUNICACIONES Y LA SEGMENTACIÓN Y SEGREGACIÓN DE REDES IT – OT

ENMARCADO EN EL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA – FINANCIADO POR LA UNIÓN EUROPEA – NEXT GENERATION EU

Donostia / San Sebastián, 20 de diciembre de 2024

ÍNDICE

1. Antecedentes 1
2. Objeto del contrato 2
2.1 Generalidades del contrato 3
3. Descripción de la situación actual 3
4. Alcance del contrato 5
4.1 Replanteo y mejora de la red de Comunicaciones 5
4.1.1 Adquisición de nuevos clúster de cortafuegos y suscripciones asociadas. 6
4.1.2 Adquisición de nuevos clúster de Switch Core y suscripciones asociadas 7
4.2 Segmentación y segregación de redes IT/OT 8
4.2.1 Resumen de tareas a realizar 9
4.2.2 Planificación 10
5. Documentación a presentar por la empresa contratista 12
6. Etiquetado verde y etiquetado digital 12
7. Principio de no causar perjuicio significativo al medio ambiente (DNSH) 12
8. Obligaciones de comunicación 13

PLIEGO DE PRESCRIPCIONES TÉCNICAS DE LA ACTUACIÓN A5.1.3 Y DE LA ACTUACIÓN A5.2.1 PARA EL REPLANTEO Y MEJORA DE LA RED DE COMUNICACIONES Y LA SEGMENTACIÓN Y SEGREGACIÓN DE REDES IT – OT

ENMARCADO EN EL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA – FINANCIADO POR LA UNIÓN EUROPEA – NEXT GENERATION EU

Componente 5, Inversión 1 del PRTR

A-5.1.3 "Replanteo y mejora de la red de comunicaciones"
A-5.2.1 "Segmentación y segregación de redes IT – OT"

1. Antecedentes

La disrupción digital ha traído consigo una creciente convergencia de TI y una creciente dependencia de la red, especialmente a medida que la movilidad y la nube eliminan muchas de las barreras relacionadas con el tiempo y el lugar en la empresa.

A medida que las organizaciones perseguimos estrategias de disrupción digital, se hace cada vez más claro que no puede haber transformación digital sin transformación de red.

La adopción de la tercera plataforma (es decir, la nube, Big Data y, movilidad) y las tecnologías de aceleración de la innovación (por ejemplo, IoT e inteligencia artificial) se basan en una red eficaz. Al mismo tiempo, están impulsando los requisitos de la red a nuevas alturas.

Con esta contratación, se pretende renovar tecnológicamente, ampliar y rediseñar la arquitectura de las actuales infraestructuras de red. Aguas del Añarbe – Añarbeko Urak, S.A. (en adelante, AGASA) cuenta con sedes dispersas en un entorno muy distribuido y con ubicaciones geográficamente distantes y en algunos casos aisladas, es por ello por lo que resulta necesario contar con una potente infraestructura de red que facilite la interconexión de los datos.

Se trata de usar las tecnologías más actuales para poder hacer llegar los datos de estaciones remotas a nuestros sistemas de control para ello nos apoyaremos en el uso redes LP-NB, 5G, … También se pretende lograr la unión de los Centros de Procesamiento de Datos (CPD) principales con fibra óptica y el replanteo de la arquitectura de red enfocándola hacia un modelo SD-WAN.

En consonancia con la nueva arquitectura de red, a través del presente contrato, se implantará una nueva segmentación y ordenación lógica de la red siguiendo la recomendación de la norma IEC 62443.

Esto así, los objetivos de la segmentación lógica de la red son los siguientes:

- Incrementar la seguridad reduciendo la superficie de ataque y dificultando los movimientos laterales.
- Mejorar el rendimiento de la propia red ya que el tráfico broadcast/multicast quedará contenido dentro de cada una de las subredes.
- Contención de los problemas de red y evitar que una falla de una subred pueda afectar a otra subred.
- Controlar el acceso a cada una de las subredes, lo cual aumenta la granularidad de quién puede acceder a qué.
- Proporcionar seguridad ante un ciberataque aislando en contenedores estancos los diferentes dispositivos críticos.

2. Objeto del contrato

En esta licitación se incluyen dos actuaciones del PERTE:

- Por un lado, el "Replanteo y mejora de la red de Comunicaciones". Esta actuación consiste en la adquisición de los equipos de red necesarios para ampliar y renovar tecnológicamente las actuales infraestructuras de red. El continuo crecimiento de aplicaciones, nodos y servicios hacen necesario ampliar los equipos de interconexión para disponer de unas mayores velocidades de trabajo y acceso a datos. Se aprovechará para modificar la arquitectura de red actual, diseñando una nueva más eficiente, más resiliente y con mayores prestaciones a la actual. Se conectarán los principales centros de datos con fibra óptica usando nuevos "switch de core" y mediante la adquisición de nuevos *firewalls* se implantará una nueva arquitectura de red enfocada hacia un modelo SD-WAN.

  Más adelante se indican los equipos instalados en cada uno de los centros y se propondrá el nuevo esquema de red a diseñar e implantar. También se ha de considerar que los equipos a suministrar deben de integrarse con algunos de los equipos de electrónica de red ya existentes y que no se van a remplazar.

- Por otro lado, la "Segmentación y segregación de redes IT/OT". En esta actuación se realizará la configuración de los nuevos equipos adquiridos con el fin implantar la nueva arquitectura de red orientada hacia un modelo SD-WAN que nos permita realizar una segmentación y ordenación lógica de la misma siguiendo las recomendaciones de la serie de normas ISA/IEC 62443.

  La nueva arquitectura de red propuesta también implica cambios de configuración en equipos ya existentes como *routers, firewalls* y *switches*, cuyas reconfiguraciones para adaptar sus enlaces a la nueva arquitectura estarán también incluidos en las labores de la presente actuación.

La importancia de que las actuaciones anteriores sean ejecutadas por la misma empresa contratista radica en varios aspectos. Por un lado, se garantiza la coherencia y compatibilidad de los equipos suministrados y configurados, evitando posibles problemas de integración o incompatibilidad. Por otro lado, se facilita la gestión y coordinación del

proyecto, al tener un único interlocutor responsable de todas las fases y tareas. Desde un punto de vista de ciberseguridad es básico este aspecto de manera que la celebración de un solo contrato minoriza los riesgos y la posibilidad de vulnerabilidades en el proceso de implantación y puesta en marcha.

De esta manera, se optimizan los recursos y los tiempos de ejecución, al evitar duplicidades o retrasos derivados de la intervención de varias empresas contratistas.

Por todo ello, el contrato no se divide en lotes debido a que el objeto del contrato implica, como se ha reflejado, la necesidad de coordinar la ejecución de diferentes prestaciones, lo que podría verse imposibilitado por la división en lotes del contrato y ejecución del mismo por varios contratistas diferentes.

2.1 Generalidades del contrato

El contratista deberá asumir todos los trabajos y suministros que sean necesarios para el correcto funcionamiento de los equipos con la configuración y programación necesarias debiendo realizar configuración de toda la red. Esto supone considerar la red en conjunto (incluyendo los equipos no suministrados en este contrato que sean propiedad de AGASA) y su configuración (VLAN, NETFLOW, SMNP, redundancia STP,…).

3. Descripción de la situación actual

A continuación, se define, a grandes rasgos, la distribución de la red actual, destacando los datos más relevantes para la ejecución del presente contrato, pero sin poder entrar en mucho detalle por motivos de seguridad. En cualquier caso, en el supuesto de considerarse necesario por parte de la empresa contratista para la correcta ejecución del contrato el conocimiento de algún dato que no haya sido facilitado a través del presente Pliego de Prescripciones Técnicas, será facilitado por AGASA, siempre y cuando el conocimiento del mismo sea indispensable para la correcta ejecución del contrato y no ponga en peligro propia seguridad de AGASA.

AGASA posee una estructura de red multisede formada por varios centros de trabajo que se conectan a una red MPLS. Algunas de las sedes cuentan además con un segundo medio de comunicación mediante una red WiMAX. Cada sede tiene su propio direccionamiento y las comunicaciones entre sedes se controlan mediante los firewalls de segmentación interna.

El acceso a Internet de todas las sedes se realiza mediante un enlace ubicado en el vCPD de ACENS y todo el tráfico entrante y saliente pasa a través de una pareja de firewalls en HA del fabricante Fortinet.

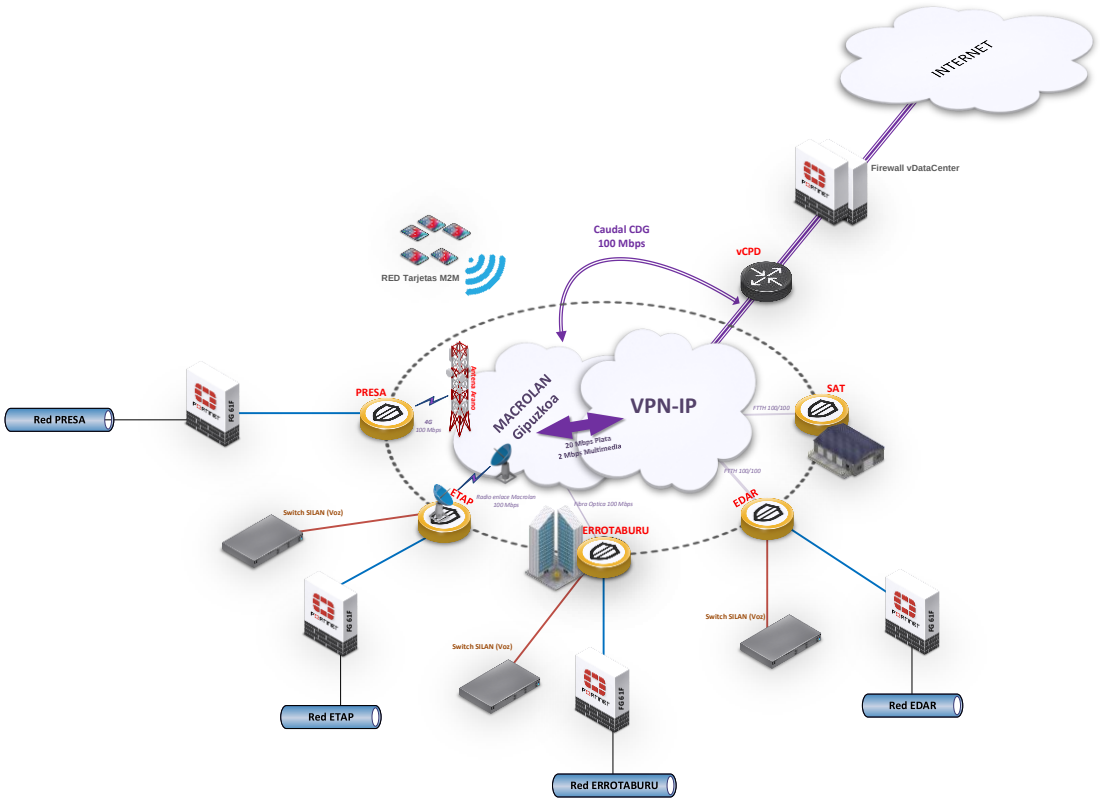
Además, en las redes internas de cada sede se cuenta con "Fortiswitches" y "FortiAPs" que son los que conectan los equipos finales en la red local.

En la sede de Errotaburu también se ubican los servidores de "Fortimanager", "FortiAnalyzer" y "FortiEMS" que permiten centralizar la gestión, el análisis y la monitorización de todos los dispositivos de seguridad de la red.

Para el tema de comunicaciones de voz se cuenta con servicio "Centrex IP" que funciona a través de la conectividad proporcionada por la "Macrolan" con caudales multimedia. Los terminales de voz de cada sede se conectan a unos switches independientes dedicados exclusivamente a este tipo de tráfico.

También se cuenta con un servicio de "conectividad gestionada M2M" que proporciona conectividad a dispositivos remotos y cubre las necesidades de control y gestión de los mismos, a través de la visualización y seguimiento en tiempo real. Las tarjetas funcionan con un APN dedicado y conectividad directa a la red MPLS que les permite comunicarse con los equipos que están en el resto de la sedes.

A continuación, mostramos un esquema general de la red de AGASA en la cual se pueden apreciar las sedes y la interconexión de estas.



Esquema general de la red de AGASA

4. Alcance del contrato

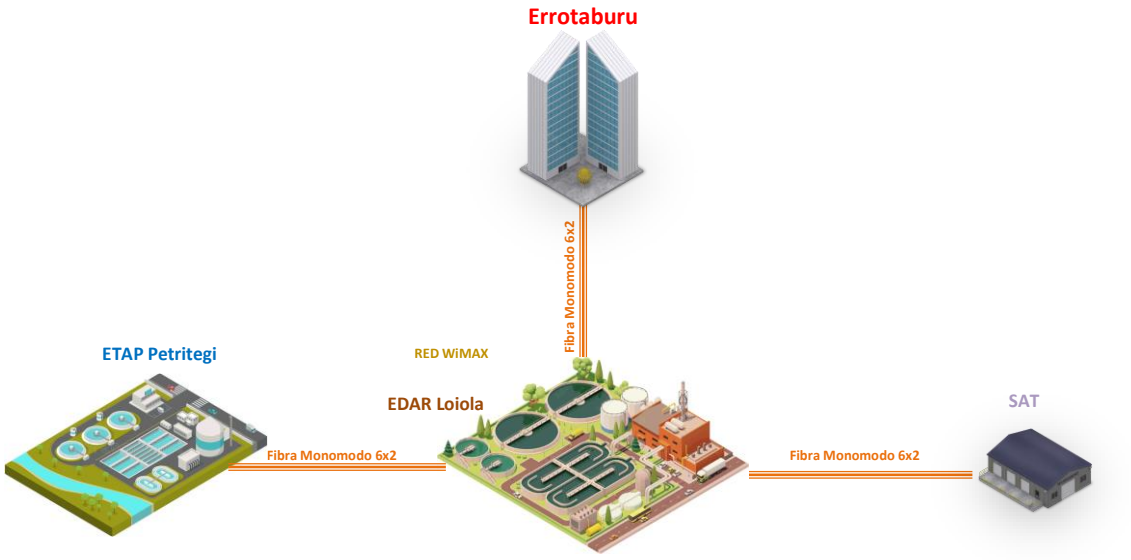
4.1 Replanteo y mejora de la red de Comunicaciones

El objeto de esta contratación es la adquisición de nuevos equipos que permitan implementar una nueva arquitectura de red basada en SD-WAN y una nueva segmentación con el fin de obtener más seguridad, control y rendimiento en la red de comunicaciones de AGASA.

Para este fin, y en una fase anterior, AGASA ha tendido de un nuevo canal de fibra óptica monomodo entre las sedes de Errotaburu, Loiola y Petritegi.

Las distancias aproximadas de las fibras son las siguientes:

- EDAR-Errotaburu 6.000 m
- EDAR-SAT 1.100 m
- EDAR-ETAP 7.200 m



Esquema de la red de comunicaciones

Teniendo en cuenta este nuevo canal de comunicación entre sedes y que pasará a ser el principal se ha hecho un rediseño de la arquitectura de red. En el nuevo esquema se pasa a un modelo basado en una red de área extensa definida por software (SD-WAN), esto es, una arquitectura de WAN virtual que permite aprovechar cualquier combinación de servicios de transporte, incluidos MPLS, LTE y servicios de Internet de banda ancha, para conectar de forma segura a los usuarios con las aplicaciones.

La primera parte para poder implantar el nuevo modelo de red consiste en la adquisición de nuevos *firewalls* y nuevos "switches de core" para las sedes de Errotaburu, Loiola y Petritegi, que trabajando de manera coordinada con el resto equipos ya existentes en

nuestra infraestructura, se encarguen de segmentar y controlar los accesos e interconexiones dentro de la propia red interna de AGASA, identificando aplicaciones, vinculando el uso de las aplicaciones a la identidad de los usuarios, realizando la prevención de amenazas y administrando las políticas de seguridad requeridas.

Se contempla la adquisición de nuevos *firewalls* y *switches* como una ampliación de la infraestructura de seguridad actual que se integre completamente con la misma, no se trata por tanto de la adquisición de un sistema independiente y aislado del actual. Esta integración, naturalmente, debido a motivos de incompatibilidad, es solo posible a través de la adquisición de equipos del fabricante que a día de hoy soporta nuestra infraestructura de seguridad, a saber, Fortinet.

Para determinar los equipos más adecuados para cada sede se han analizado las necesidades de la red y las características de los modelos del fabricante. Se ha tenido en cuenta el número de usuarios, el ancho de banda requerido, el tipo de tráfico y las funcionalidades de seguridad que se desean implementar. De esta forma, se ha optado por unos modelos concretos que ofrecen las prestaciones mínimas necesarias para garantizar el rendimiento y la protección de la red.

Según lo indicado en los apartados anteriores, son objeto del contrato el suministro los equipos y los posteriores servicios que se enumeran en las siguientes Cláusulas:

4.1.1 Adquisición de nuevos clúster de cortafuegos y suscripciones asociadas.

Sede Errotaburu

- 2 cortafuegos Fortigate 120G.
- 2 suscripciones FortiCare Premium para 3 años.
- 2 Suscripciones Fortiguard Unified Threat Protection (UTP) para 3 años.
- Transceptores SFP de unión de los dos FortiGate 120 con los FortiSwitch-T1024E: 4x FN-TRAN-SFP+GC.

Sede Loiola

- 2 cortafuegos Fortigate 120G.
- 2 suscripciones FortiCare Premium para 3 años.
- 2 suscripciones Fortiguard Unified Threat Protection (UTP) para 3 años.
- Transceptores SFP de unión de los dos FortiGate 120 con los FortiSwitch-T1024E: 4x FN-TRAN-SFP+GC.

Sede Petritegi

- 2 cortafuegos Fortigate 120G.
- 2 suscripciones FortiCare Premium para 3 años.
- 2 Suscripciones Fortiguard Advanced Threat Protection para 3 años.
- Transceptores SFP de unión de los dos FortiGate 120 con los FortiSwitch-T1024E: 4x FN-TRAN-SFP+GC.

4.1.2 Adquisición de nuevos clúster de Switch Core y suscripciones asociadas.

Sede Errotaburu

- 2 Switches FortiSwitch-T1024E.
- 2 Suscripciones FortiCare Premium para 3 años.
- Transceptores SFP de unión de los dos FortiSwitch-T1024E con los Fortiswitch de acceso: 4x FN-TRAN-SFP+GC.
- Transceptores SFP 40 Gb para la unión de los FortiSwitch-T1024E entre sedes: 2x FN-TRAN-QSFP+LR (monomodo).

Sede Loiola

- 2 Switches FortiSwitch-T1024E.
- 2 Suscripciones FortiCare Premium para 3 años.
- Transceptores SFP de unión de los dos FortiSwitch-T1024E con los Fortiswitch de acceso: 4x FN-TRAN-SFP+GC.
- Transceptores SFP 40 Gb para la unión de los FortiSwitch-T1024E entre sedes: 2x FN-TRAN-QSFP+LR (monomodo).

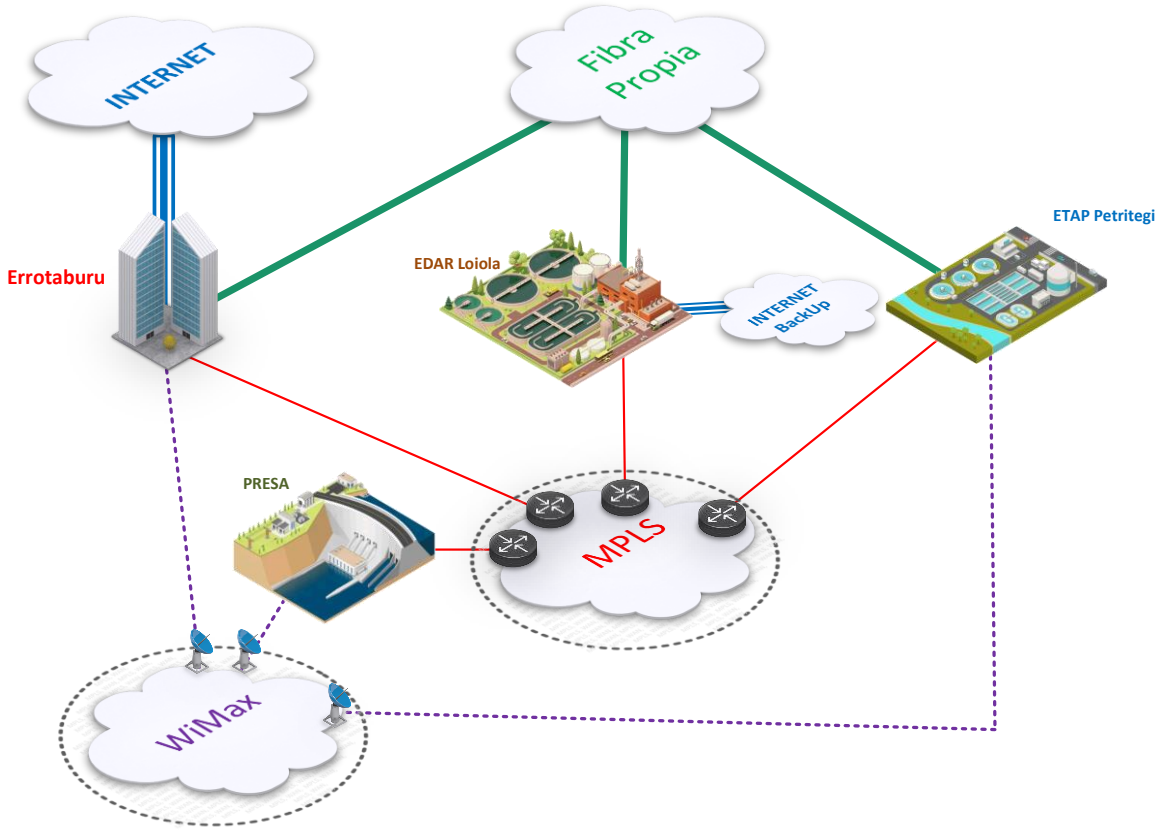
Sede Petritegi

- 2 Switches FortiSwitch-T1024E.
- 2 Suscripciones FortiCare Premium para 3 años.
- Transceptores SFP de unión de los dos FortiSwitch-T1024E con los Fortiswitch de acceso: 4x FN-TRAN-SFP+GC.
- Transceptores SFP 40 Gb para la unión de los FortiSwitch-T1024E entre sedes: 4x FN-TRAN-QSFP+LR (monomodo).

4.2 Segmentación y segregación de redes IT/OT

El objetivo de esta contratación es la instalación y configuración de los equipos adquiridos para migrar la red de AGASA a un nuevo esquema de red basado en una arquitectura de red basada en SD-WAN que permitirá aprovechar los diferentes canales de acceso disponibles: la MPLS, el WIMAX y la nueva fibra óptica. Por lo tanto, se deberá realizar la configuración de los equipos tanto de los nuevos como de los que no se sustituirán para poder soportar la nueva arquitectura de red propuesta.

La migración a una arquitectura de red basada en SD-WAN (*Software Defined Wide Area Network*) permitirá aprovechar las ventajas de la virtualización y la automatización de los servicios de red, reduciendo los costes operativos y mejorando la agilidad y la escalabilidad.



Para realizar la migración a la nueva arquitectura de red basada en SD-WAN, la idea planteada es montar en las sedes de Errotaburu, Loiola y Petritegi dos "*switches core*" formando un *stack* virtual. A su vez estos *switches* se conectarán mediante fibra óptica entre las tres sedes.

Por otro lado, en cada una de las tres sedes anteriormente citadas se montarán dos *firewalls* en configuración HA (*High Availability*), filtrarán el tráfico entrante y saliente de las redes, y que pueden funcionar en modo activo-pasivo o activo-activo, garantizando la continuidad

del servicio en caso de fallo de uno de ellos. Los firewalls permitirán la segmentación de la redes IT/OT definiendo zonas de seguridad y políticas de acceso de acuerdo con las necesidades de la empresa.

El acceso a internet que actualmente pasa por los *firewalls* situados en el vCPD de Acens se eliminará y se proporcionarán por parte de AGASA dos nuevos canales de acceso a internet en dos de las sedes (Errotaburu y Loiola), uno actuará como principal y otro como canal de respaldo. Con esto se eliminarán los dos firewalls y la salida a internet situada en Acens.

Todo lo anterior implica cambios en la configuración de la red, tanto a nivel de la LAN como de la WAN. La salida a internet se hará directamente desde las sedes de Errotaburu y Loiola, sin pasar por el vCPD de Acens, lo que supone una mejora en la latencia y el ancho de banda. Los routers de la MPLS, que actualmente conectan las sedes se integrarán con los firewalls y los switches mediante protocolos estándar, como OSPF o BGP, y se configurarán para garantizar la calidad de servicio y la seguridad de las comunicaciones.

Una vez realizada esta migración, la nueva arquitectura nos permitirá segmentar la red en diferentes dominios lógicos, según el tipo de tráfico y las necesidades de cada zona. Cada uno de ellos tendrá una configuración específica de seguridad, enrutamiento y calidad de servicio, que se aplicará mediante políticas centralizadas y distribuidas por los equipos Fortinet.

De esta forma, se logrará una mayor visibilidad, control y protección de la red, así como una optimización del rendimiento y la disponibilidad de los recursos.

4.2.1 Resumen de tareas a realizar

Para lograr la arquitectura de red propuesta se han de realizar al menos las siguientes tareas:

- Diseño e implantación un nuevo esquema de red basado en SD-WAN en el cual las diferentes sedes puedan comunicarse usando diferentes caminos (MPLS, Fibra Propia entre sedes, WIMAX,…). Tenemos las sedes de Errotaburu, Loiola, Petritegi, Presa, ACENS y las M2M.

- Configuración de las reglas de SD-WAN que permitan definir el canal o canales por los que se enviará cada flujo de tráfico.

- Configurar la nueva salida a Internet eliminando la situada actualmente en el vCPD de ACENS y haciendo que se salga a internet por una de las sedes (Errotaburu) con *backup* alternativo en otra de las sedes (Loiola).

- Al eliminar el firewall perimetral situado en ACENS habrá que migrar elementos de su configuración como los siguientes:

    - Políticas
    - Usuarios

  - Certificados
  - *Fortitokens*
  - Configuraciones de NTP, DNS, DHCP,…
  - Migrar las VLAN existentes.

- Al crear una nueva arquitectura de red con nuevos firewalls y nuevos switches tendremos que configurar el "Security Fabric" de Fortinet, integrando todos los *fortigates, fortiswitches, fortiaps* y el *Fortianalizer, Fortimanager y FortiEMS*.

- En cuanto a otros temas referentes a la configuración de los *fortigate* tendremos que:

  - Proceder a la instalación y puesta en marcha, siguiendo las configuraciones recomendadas por fabricante, tales como: configuración de acceso a la red, configuración de la *interface*, *hostnames*, ajustes de los DNS, servidor de actualización y servidor PROXY, *Network Time Protocol* (NTP), verificación e instalación de nuevas versiones de software y cambio de contraseña para administradores. Todas las configuraciones anteriores se basarán en parámetros proporcionados por AGASA en el momento de la instalación.
  - Registro del cortafuegos con el servicio de soporte de fabricante.
  - Activación de las licencias pertinentes.
  - Configurar "Deep packet inspection".
  - Configurar la VPN para acceso externo.
  - Integración con nuestro directorio activo de modo que nos permita desplegar políticas de seguridad específicas para el usuario detectado.
  - Configuración HA de los equipos suministrados. Definición de las condiciones de balanceo.
  - Creación de perfiles de seguridad según las mejoras prácticas del fabricante.

- Creación de las zonas de seguridad en los firewalls, (Servidores, equipos IT, DMZ, Externa, DMZ Interna, PLCs, SCADAs, CCTV, Control de Accesos,…), la configuración de dichas zonas será facilitada por AGASA.

- Integrar los nuevos firewals y switchs en los "Fortianalizer" y "Fortimanager" ya presentes en la red.

4.2.2 Planificación

Para la realización de las referidas tareas se han estimado las siguientes fases:

1. **Estudio previo de la infraestructura de red existente**

   Estudio en alto nivel de la infraestructura actual, para ello se proporcionará al contratista la información necesaria.

2. **Reunión de arranque**

En la reunión se revisará el alcance de la contratación y se detallarán las características del equipamiento a suministrar y de los servicios a realizar por si se le plantearan dudas a alguna de las partes contratantes (esto es, a la empresa contratista o a la entidad contratante). Como resultado de esta reunión, se acordarán los requisitos, planificación y equipo de trabajo que serán tenidos en cuenta en el resto de la duración del contrato. En cualquier caso, lo acordado en la referida reunión no contravendrá lo propuesto por la empresa contratista.

También se identificará en esta reunión la información a aportar por parte de AGASA para poder continuar con las siguientes tareas del contrato, como pueden ser:

- Identificación de los objetivos sobre la infraestructura a desplegar.
- Mapa de red L1, L2 y L3 donde se ubicará la infraestructura.

En esta reunión AGASA facilitará la configuración y políticas del equipamiento actual situado en Acens que se va a sustituir por el nuevo equipamiento adquirido en el concurso para ir avanzando en el estudio y la migración de las mismas.

3. **Elaboración del plan de diseño e implantación de la red SD-WAN.**

   Consistirá en la elaboración de un plan de diseño e implantación de la nueva red SD-WAN, que incluya los diagramas de red, las tablas de ruteo, los perfiles de seguridad, las políticas de acceso, los puntos de gestión centralizada, plan de pruebas que incluirá, al menos, pruebas sobre la arquitectura y la funcionalidad del equipamiento desplegado …

4. **Configuración e instalación de los nuevos "firewalls y switchs de core".**

   Siguiendo el plan de diseño e implantación y asegurando la compatibilidad y la interoperabilidad con los equipos existentes.

5. **Preparación de la documentación necesaria para la migración.**

   Todo trabajo que suponga un corte del servicio se deberá planificar y comunicar a AGASA, por adelantado, con al menos, 15 días de antelación a la fecha en los que se realicen los mismos, y en caso de que AGASA así lo decida, deberá realizarse fuera de la jornada laboral de AGASA (siendo la jornada laboral de lunes a viernes de 7:30 a 16:00).

6. **Labores de enracado de equipos y cableado.**

   El contratista contará con la colaboración del personal de AGASA para coordinar las tareas de ubicación, enracado, cableado, etc., de los equipos físicos, sobre la actual infraestructura de AGASA.

7. **Configuración de los dispositivos.**

Será necesario preparar los nuevos equipos de electrónica de red para la nueva arquitectura de red, adecuando parte de la configuración de los equipos actuales y añadiendo nuevas funcionalidades solicitadas por AGASA.

8. **Puesta en marcha y verificación.**

   Realización de las pruebas de verificación y validación de la red SD-WAN con segmentación IT/OT, comprobando el correcto funcionamiento de la conectividad, la seguridad, el rendimiento y la disponibilidad de la red.

5. Documentación a presentar por la empresa contratista

La documentación requerida a la finalización del despliegue de la nueva red debe contener, al menos:

- Diagrama físico (formato Visio o similar).
- Documentación del proceso de despliegue y las configuraciones aplicadas en cada fase.
- Reporte de las pruebas realizadas para la validación del correcto funcionamiento de HA y otras pruebas realizadas.
- Inventario de licencias y mantenimiento en vigor.

La empresa contratista deberá entregar la documentación referida en la presente Cláusula en el plazo máximo de un mes desde la firma del acta de finalización del contrato.

6. Etiquetado verde y etiquetado digital

Esta actuación contribuye de manera directa a la transición ecológica. En concreto, se incluye en la etiqueta climática Nº 041bis, incluida en el Anexo VI del Reglamento de Recuperación y Resiliencia, contribuyendo con un 40% a los objetivos climáticos y un 100% a los objetivos ambientales. No obstante, no contribuye de manera directa a la transición digital.

7. Principio de no causar perjuicio significativo al medio ambiente (DNSH)

El contratista y los posibles subcontratistas garantizarán el respeto al principio de «no causar un perjuicio significativo» (DNSH), exigido por el REGLAMENTO (UE) 2021/241, por el que se establece el Mecanismo de Recuperación y Resiliencia y el artículo 17 del Reglamento (UE) 2020/852 del Parlamento Europeo y del Consejo de 18 de junio de 2020 relativo al establecimiento de un marco para facilitar las inversiones sostenibles y por el que se modifica el Reglamento (UE) 2019/2088. En particular se cumplirá con la Comunicación de la Comisión Guía técnica 2021/C 58/01, sobre la aplicación del principio de «no causar un perjuicio significativo».

A estos efectos, deberán suscribir una declaración responsable, como la que figura a modo de Anexo en la Carátula de la presente licitación sobre el cumplimiento de "no causar un perjuicio significativo" (DNSH) a los 6 objetivos medioambientales en el sentido del Artículo 17 del Reglamento (UE) 2020/852.

Deberán prestar especial atención al cumplimiento del siguiente criterio:

Los equipos utilizados no contendrán las sustancias restringidas enumeradas en el anexo II de la Directiva 2011/65/UE, excepto cuando los valores de concentración en peso en materiales homogéneos no superen los enumerados en dicho anexo.

El contratista deberá aportar:

"1. Marcado CE de los equipos.
2. En su defecto, ficha técnica donde se pueda comprobar el cumplimiento de la norma a verificar."

8. Obligaciones de comunicación

La entidad contratista y subcontratistas, si fuera el caso, estarán obligadas a cumplir las obligaciones de información y publicidad establecidas en el Artículo 9. Comunicación, de la Orden HFP/1030/2021, de 29 de septiembre, por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia.

Concretamente, estarán obligados a cumplir las siguientes obligaciones:

a) En los documentos de trabajo, así como en los informes y en cualquier tipo de soporte que se utilice en las actuaciones necesarias para el objeto del contrato, deberá exhibirse de forma correcta y destacada el emblema de la UE con una declaración de financiación adecuada que diga "financiado por la Unión Europea - NextGenerationEU", junto al logo del PRTR y contener tanto en su encabezamiento como en su cuerpo de desarrollo la siguiente referencia «Plan de Recuperación, Transformación y Resiliencia - Financiado por la Unión Europea – NextGenerationEU».

b) En las medidas de información y comunicación, sea cual fuere el canal de comunicación que se emplee, se deberá a hacer referencia a que la inversión está financiada por la Unión Europea a través del Mecanismo de Recuperación y Resiliencia-NextGeneration EU, instrumento financiero de la inversión C5.I1. «Materialización de actuaciones de depuración, saneamiento, eficiencia, ahorro, reutilización y seguridad de infraestructuras» del Plan de Recuperación, Transformación y Resiliencia.

c) El órgano de contratación proporcionará durante la ejecución del contrato las indicaciones acerca del contenido preciso en cada medio y/o formato.

d) Cuando proceda, se indicará la siguiente cláusula de exención de responsabilidad: «Financiado por la Unión Europea - NextGenerationEU. Sin embargo, los puntos de vista y las opiniones expresadas son únicamente los del autor/a o autores y no reflejan necesariamente los de la Unión Europea o la Comisión Europea. Ni la Unión Europea ni la Comisión Europea pueden ser consideradas responsables de las mismas».