PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES

SUMINISTRO, INSTALACION, PUESTA EN MARCHA Y MANTENIMIENTO DE UNA ARQUITECTURA DE SEGURIDAD Y REDES EN LA NUBE BASADA EN EL MODELO SASE PARA EL ACCESO REMOTO SEGURO A RECURSOS INTERNOS DEL CABB MEDIANTE ZTNA, FINANCIADO CON FONDOS PROCEDENTES DEL MECANISMO PARA LA RECUPERACIÓN Y RESILENCIA NEXT GENERATION EU EN EL MARCO DEL COMPONENTE 5 "PRESERVACIÓN DEL LITORAL Y RECURSOS HÍDRICOS" INVERSIÓN 3 DENOMINADA «TRANSICIÓN DIGITAL EN EL SECTOR DEL AGUA (ENFORCEMENT DIGITAL MEDIOAMBIENTAL)

Índice

1 OBJETO DEL PROYECTO.

El Consorcio de Aguas Bilbao Bizkaia, en adelante CABB, en concordancia con el constante avance tecnológico y transformación digital, pretende evolucionar su solución tradicional de VPN de acceso remoto a un nuevo tipo de tecnología más moderna que, entre otros, permita mejorar la experiencia de usuario y aumentar la eficiencia y seguridad de las conexiones remotas con independencia de su ubicación y los servicios a los que se conecte.

El CABB pretende desplegar y probar una arquitectura de red basada en el modelo SASE (Secure Access Service Edge) con funcionalidades de seguridad específicas de ZTNA (Zero Trust Network Access) combinadas con SWG (Secure Web Gateway) que en un futuro cercano puedan reemplazar en su totalidad la solución tradicional actual de VPN del CABB y que además permita una evolución de la arquitectura hacia otros servicios que también ofrece el modelo SASE como CASB (Cloud Access Security Broker), DLP (Data Loss Prevention) o similares, previa adquisición del licenciamiento correspondiente que de momento queda fuera del alcance del presente pliego.

A rasgos generales los objetivos que se pretenden con el presente proyecto son:

1. Implantar y probar, como mínimo, los servicios ZTNA y SWG del modelo SASE con un licenciamiento mínimo de 200 usuarios en sustitución de parte de la solución actual de la VPN tradicional del CABB.
2. Integración de la arquitectura de red SASE con:
    a. los servicios de monitorización internos del CABB
    b. los servicios de monitorización externos del CABB (NOC y SOC)
3. Servicio de mantenimiento de la arquitectura por parte de fabricante e integrador en modalidad 24x7x4 durante toda la duración del contrato.
4. Servicio de Asistencia técnica especializada de fabricante de la solución para:
    a. Confirmación y validez de la solución implementada
    b. Seguimiento, propuestas de evolución y mejoras de la solución en base a las particularidades de la arquitectura del CABB
5. Servicio de Bolsa de Horas de Asistencia técnica especializada de integrador en las tecnologías del proyecto por una duración de 25 horas al año.
6. Documentación
7. Formación

2 DESCRIPCIÓN Y ALCANCE

El proyecto se considera “llave en mano”, acometiendo el contratista todos los trabajos y suministros que sean necesarios para el correcto funcionamiento de los equipos con la configuración y programación necesarias dando respuesta como mínimo a todos los puntos indicados en el apartado 1 del presente documento.

Se deberá realizar la instalación y configuración de todo equipamiento nuevo teniendo en cuenta el resto de la red e infraestructura del CABB, esto supone considerar la red como un todo (incluyendo los equipos no suministrados en este contrato) y su configuración (VLAN, netflow, SMNP, redundancia STP, monitorización, etc.) para que funcione y sea compatible con nuevos los equipos instalados, siguiendo las especificaciones, consideraciones y necesidades del CABB. Se deberá indicar y valorar todo elemento que se considere necesario para el correcto funcionamiento de la red según las prescripciones indicadas e incluso las que no se hayan contemplado en este Pliego indicándose en la oferta.

En la oferta técnica presentada por el licitador será obligatorio presentar la misma tabla resumen del equipamiento ofertado presentada en la oferta económica descrita en el apartado 7 del presente documento,

donde se especifiquen para los equipos, licencias y software ofertados sus referencias, descripciones y número, pero sin incluir ningún importe económico.

El proyecto incluye el suministro, documentación, configuración, instalación, migración, puesta en marcha, formación, mantenimiento y posterior asistencia técnica del equipamiento y sistemas que conciernen a dicho proyecto.

A continuación, se detallan consideraciones generales importantes a tener en cuenta en las fases, tareas e hitos descritos en el apartado 1 del presente documento.

2.1 Análisis y diseño previo de la solución

Debido a la diferencia tecnológica existente entre las soluciones tradicionales de VPN y las actuales arquitecturas de SASE, el CABB considera imprescindible como primer paso a ejecutar por parte del licitador, en colaboración con el CABB y siguiendo las premisas del fabricante de la solución, la realización de un análisis y replanteo previo de la situación actual de la solución VPN del CABB y conocer el mejor método de evolución hacia la nueva arquitectura SASE.

El licitador deberá comenzar este análisis previo, salvo por solicitud expresa del CABB, en un plazo máximo de 1 semana después de la firma de contrato.

Tras la finalización de este análisis el licitador deberá presentar al CABB como mínimo la siguiente información en un plazo máximo de 3 semanas desde el comienzo del análisis previo, salvo por solicitud expresa del CABB:

- Servicios y funcionalidades a definir en la nueva arquitectura SASE adaptada a las particularidades del CABB para dar servicio a las conexiones remotas según sus especificaciones.
- Posibles mejoras y nuevos servicios a adquirir en un futuro en función de las posibilidades y licencias que ofrece la solución SASE.
- Plan de migración (a ejecutar por el licitador) de los usuarios propuestos por el CABB para pasar de la actual solución VPN tradicional a la nueva arquitectura SASE basada en ZTNA con SWG.
- Plan de pruebas y redundancia de la solución.
- Otra información relevante a aportar por el licitador y/o fabricante relativa a la arquitectura SASE.

2.2 Suministro

El suministro comprende la entrega de todo el equipamiento, software y licenciamiento o similar necesarios para que la instalación y el servicio quede en funcionamiento de acuerdo con este PPTP.

Todo lo incluido en la oferta por parte del licitador debe ser perfectamente compatible con el equipamiento disponible actualmente por el CABB.

Cuando proceda, el equipamiento nuevo deberá entregarse con la imagen y versiones del resto de equipos del CABB, indicadas en el Pliego o las que se especifiquen en el momento de la entrega del material por parte del personal responsable del contrato del CABB y/o recomendadas por el fabricante. No obstante, en caso de que en el momento de la implantación se detecte que, por necesidades de funcionalidades o seguridad, sea necesaria la actualización a una versión superior, el licitador será encargado de la actualización tanto de los equipos suministrados como de los equipos en producción directamente relacionados con el proyecto, sin sobrecosto alguno para el CABB.

Salvo petición expresa del CABB, se considera 1 semana después de la firma de contrato como plazo máximo para realizar la reunión de lanzamiento del proyecto en la que se definirá los equipos y métodos de trabajo y los siguientes plazos cuando proceda:

- Plazo máximo para la realización por parte del licitador del pedido de compra del nuevo equipamiento licenciamiento, y/o mantenimiento al fabricante, incluidas las renovaciones:
    - El CABB, para aquellos casos de urgencia y en los que no sea necesario un replanteo específico de las instalaciones para determinarlo, podrá exigir que el licitador lance el pedido de compra con el fabricante el mismo día de la reunión.
    - En condiciones normales, en la reunión inicial del proyecto se planificará la fecha de lanzamiento de la compra con el fabricante en función de las características particulares de cada proyecto y teniendo en cuenta aspectos como:
        - Estimaciones de fechas de entrega por parte de fabricante de equipamiento, licenciamiento y mantenimientos.
        - Estimación de duración de los trabajos previos de ingeniería necesarios a ejecutar antes de la nueva instalación.
        - Estimación de fechas de posibles replanteos previos a las instalaciones necesarios para determinar equipamiento y/o licenciamiento específico
        - Previsión de fechas de puesta en producción

Será obligatorio, en caso de solicitud expresa por parte del CABB, la presentación de la documentación o una notificación oficial por parte del fabricante que acredite el lanzamiento del pedido de compra por parte del licitador.

El plazo máximo de entrega del material en condiciones de mercado normales debe ser de 4 semanas a partir del lanzamiento del pedido según lo acordado en la reunión inicial del proyecto, debiendo el contratista asumir la responsabilidad de fechas de entrega del o los fabricantes. La demora o incumplimiento de alguno de estos plazos supone la posibilidad de aplicar penalizaciones contempladas en el pliego administrativo del presente proyecto, pudiendo incluso implicar la rescisión del contrato.

En caso de situaciones fuera de lo común (huelga prolongada de transporte, escasez de componentes para la fabricación de los equipos o algún problema grave, debidamente justificado ante el CABB, que pueda afectar a contratistas, fabricantes o intermediarios) que puedan derivar en retrasos mayores en la entrega y/o la renovación del mantenimiento o licencias y que originen una situación crítica para el CABB (disponer en producción de equipos sin mantenimiento por parte del fabricante o en fuera de vida, la no renovación del mantenimiento y/o licencias de equipos del CABB en producción o retrasos superiores a 4 meses en la ejecución del proyecto) podrán implicar, dependiendo de la situación fuera de lo común y sus consecuencias, la rescisión del contrato o el planteamiento de una solución alternativa con otro equipamiento del mismo u otro fabricante.

Será obligación de la empresa adjudicataria la realización de diferentes pedidos parciales con los distintos fabricantes para poder disponer de equipamiento que permita avanzar con el proyecto sin la necesidad de tener que esperar al envío completo por parte del fabricante de todo el equipamiento adquirido. Por ejemplo, si en el pedido se contempla la adquisición de 16 equipos y el fabricante sólo dispone de una parte de los mismos y está a la espera de la recepción del resto, el CABB, dependiendo de la planificación y fechas de recepción del pedido completo, podrá exigir la entrega parcial de parte del equipamiento para avanzar en el proyecto. Otro ejemplo puede ser la solicitud a un fabricante de diferentes modelos de equipos, por los que se podrá solicitar la entrega de uno de los modelos sin tener que esperar a la recepción completa de todos los

modelos adquiridos en el caso de que algunos de los mismos tengan retrasos que impidan el avance del proyecto.

Todo equipamiento ofertado deberá ser nuevo y original del fabricante (tanto equipos activos como equipos pasivos tipo transceptores ópticos), siendo motivo de exclusión del concurso la inclusión de cualquier material no original del fabricante.

El CABB debe aparecer como propietario del equipamiento suministrado y debe constar como tal en las bases de datos del fabricante de dicho equipamiento.

En el caso de que alguno de los equipos (incluido ópticas, cables, memorias y demás componentes similares solicitados en los casos que proceda) tuviera anunciado el fin de soporte por parte del fabricante durante la duración del contrato, el licitador deberá realizar su oferta incluyendo el equipamiento propuesto por el fabricante para su sustitución.

El presente proyecto debe incluir cualquier configuración necesaria para implementar las funcionalidades requeridas, así como cualquier otro elemento de la red necesario para el sistema quede funcionando plenamente y cumpla los requisitos solicitados en el presente pliego.

2.3 Asistencia técnica para la implantación de la arquitectura SASE

El presente proyecto debe incluir el servicio de Asistencia Técnica especializada necesaria para implementar las funcionalidades requeridas en el pliego, según lo indicado en los apartados 1 y 2.1 del presente documento con licenciamiento hasta para 200 usuarios totales.

A la hora de la valoración y el esfuerzo por parte del licitador, será necesario como mínimo dar servicio a las siguientes funcionalidades para los usuarios remotos en la nueva arquitectura SASE basada en ZTNA con SWG, completadas y más detalladas en el apartado 6 del presente documento:

1. Capacidad de la solución para realizar un túnel IPSEC contra la nube de la solución de SASE desde los FWs perimetrales del CABB con conexión a INTERNET y sin necesidad de la instalación de máquinas virtuales dentro de la red corporativa del CABB que realicen las funciones de concentradores y/o conectores entre la nube de la solución SASE y la red corporativa del CABB.
2. Autenticación de todos los clientes contra la solución contra Azure AD y con doble factor de autenticación.
3. Geolocalización y control de las ubicaciones/nodos de conexión desde donde se permiten las conexiones de los clientes remotos.
4. Necesidad de configuración de un mínimo de 2 tipos de accesos remotos genéricos principales para los usuarios actuales de VPN:
    a. Conexión remota CON agente software con los siguientes requerimientos mínimos:
        i. Basada en la instalación remota para el CABB del software de cliente pesado específico de la solución SASE en los equipos corporativos del CABB (Windows, MAC OS, Android e IOS).
        ii. La actualización e instalación de dicho cliente se podrá ejecutar de forma transparente y automática desde la consola centralizada de la solución SASE o desde los propios equipos sin necesidad de hacerlo de forma manual.
        iii. Cada cliente dispondrá de un direccionamiento IP específico dentro de un rango de direccionamiento privado proporcionado por el CABB y el acceso determinado por las políticas actuales definidas en los concentradores VPN actuales y FWs perimetrales del CABB.

iv. El agente software detectará cuando el usuario NO esté conectado a la red corporativa y sólo activará la conexión ZTNA en ese caso, activando también un control de navegación basado en las políticas de SWG definidas similares a las de la red corporativa.
v. Control de conexiones remotas de los clientes, basadas en políticas de cumplimiento del dispositivo final como certificados propios, versiones y estados de EPDRs…
vi. Otras funcionalidades de seguridad extra que pueda proporcionar la solución para estos tipos de accesos.

b. Conexión remota SIN agente software con los siguientes requerimientos mínimos:
i. Publicación de accesos remotos basados en SSH, RDP, VNC mediante navegador.
ii. En lo que respecta a los accesos RDP, se dispondrá de la capacidad de soportar teclado en español y permitirá la utilización de múltiples pantallas. Además, incluirá funcionalidades de grabación de sesiones, que facilitará la investigación de eventos que puedan ocurrir durante la sesión
iii. Publicación de aplicaciones WEB internas del CABB, especificando en la definición de la misma, la URL completa compuesta tanto por el hostname del servidor donde se aloja y como por el path dentro de dicho servidor (no serán válidas aquellas soluciones SASE que sólo puedan definir el hostname del servidor donde se aloja y NO puedan incluir el path)
iv. Control de las publicaciones anteriores especificando permisos para copiar, pegar, subir y/o descargar archivos
v. Otras funcionalidades de seguridad extra que pueda proporcionar la solución para estos tipos de accesos.

5. Generación de toda la configuración necesaria en la arquitectura SASE para la definición de los accesos remotos previamente especificados y delimitados según las necesidades y especificaciones del CABB para un máximo de 200 usuarios, solicitando también la configuración de políticas en función de grupos definidos en Azure AD y sincronizados con la solución SASE.
6. Configuración y migración de los usuarios de forma transparente en sus dispositivos finales de conexión para el funcionamiento de la solución.
7. Documentación de migración, plan de pruebas y plan de redundancia y manuales de usuario para la conexión remota a la nueva arquitectura de red SASE.
8. Puesta en marcha de los diferentes accesos para los usuarios de forma escalonada según los requerimientos del CABB

2.3.1 Proceso de migración

Otro aspecto importante a considerar por parte del licitador son los trabajos a realizar y las fases de migración a ejecutar en la puesta en marcha de los diferentes accesos para los usuarios de forma escalonada, teniendo en cuenta que, como mínimo, el proyecto debe constar de las siguientes fases:

1- Configuración, preparación y puesta en marcha de la solución, preparación de documentación y manuales
   a. Se considera un periodo máximo de 4 semanas para esta fase
2- Migración de usuarios VPN tradicionales con un mínimo de las siguientes fases (con un intervalo estimado de 1 semana entre fases, aunque puede que en las primeras fases se decida ampliar el tiempo para confirmar el correcto funcionamiento de la solución)
   a. Fase 1: Migración de usuarios VPN corporativos del departamento de Informática CON agente software
   b. Fase 2: Migración de usuarios VPN corporativos del departamento de Informática SIN agente software

c. Fase 3: Migración de usuarios VPN de ciertas empresas colaboradoras del CABB a determinar CON y SIN agente software
d. Fase 4: Migración de usuarios VPN corporativos de ciertos departamentos del CABB a determinar CON y SIN agente software
e. Fase 5: Migración de usuarios VPN corporativos de ciertos departamentos a determinar CON y SIN agente software
f. Fase 6: Migración de usuarios VPN de ciertas empresas colaboradoras del CABB a determinar CON y SIN agente software

Entre las tareas de cada fase de migración de usuarios VPN tradicionales es importante que además de preparar la configuración necesaria en la arquitectura SASE, será también responsabilidad del licitador, siguiendo siempre las directrices del CABB:

1- Preparación y comprobación de la correcta configuración SASE particular necesaria para la migración de cada usuario.
2- Envío de manual e invitaciones correspondiente de uso por correo electrónico a cada usuario, días previos a la migración.
3- Confirmación de la correcta instalación del agente software y lanzamiento de la instalación/actualización remota previa necesaria para cada usuario.
4- Teléfono de contacto y atención telefónica posterior a la migración para resolución de posibles problemas puntuales y fallos de conexión de usuarios migrados con anterioridad, teniendo en cuenta el horario laboral del CABB

2.4 Integración de la nueva arquitectura SASE con los sistemas de monitorización del CABB

2.4.1 Sistemas de monitorización internos

- Servidor Syslog. El CABB dispone de un servidor syslog interno que recoge logs de los concentradores VPN actuales para:
  - Almacenar y consultar logs de forma centralizada
  - Generación de correos de eventos de alarma ante la recepción de determinados logs
  - Elaboración de informes con los logs recogidos
- Servidor SNMP. El CABB dispone también de un servidor interno de monitorización mediante ICMP y SNMP v3 que realiza polling a los servidores VPN actuales para:
  - Conocer su estado
  - Generación de correos de eventos de alarma ante la recepción de posibles fallos

La nueva solución de ZTNA+SWG basada en arquitectura SASE debe poder integrarse en ambas soluciones y el presente pliego incluye los trabajos del integrador para dicha integración y puesta a punto según las indicaciones de particulares del CABB y valores habituales de monitorización de la arquitectura .

En caso de incompatibilidad con alguno de los servidores internos del CABB, el integrador será el encargado de hacerse cargo de todos los gastos que puedan generar sin coste alguno para el CABB, incluida la implantación e integración vía API si fuera necesario.

2.4.2 Sistemas de monitorización externos

- NOC. El CABB dispone de un servicio de monitorización en una empresa externa en la que un tercero monitoriza mediante ICMP y SNMP y la herramienta de NAGIOS las variables de PING, BW, estado de interfaces, memoria, CPU… de los concentradores VPN actuales para que, en caso de recepción de

alguna alarma y previa elaboración de un procedimiento de actuación, se pone en marcha un proceso de respuesta y actuación ante alarmas específicas que pueden afectar la producción.

- SOC. El CABB está en proceso de implantación de un servicio de monitorización de amenazas de seguridad (SOC) junto con una oficina de cliente para actuación ante las mismas.

Será necesario por parte del licitador proporcionar una propuesta de adaptación de ambos modelos de monitorización (SOC y NOC) para la nueva arquitectura SASE, incluida la implantación e integración vía API si fuera necesario.

2.4.3 Registro de logs y generación de informes

La nueva solución deberá asegurar el registro de logs de acceso de los usuarios para su consulta y permitir la generación de informes específicos según las necesidades del CABB

2.5 Servicio de Mantenimiento

Para llevar a cabo el mantenimiento o soporte se requiere como mínimo de un servicio que comprenderá:

- Resolución de averías insitu o en remoto 24 horas cualquier día del año (24x7) por parte del integrador para toda la duración del contrato.
- Servicio de mantenimiento 24x7 del fabricante para toda la duración del contrato.

Se deberá prestar soporte durante la duración del contrato para todos los componentes hardware, software y licencias ofertados, tanto por el fabricante como por el licitador en las condiciones previamente indicadas.

A la hora de contratar el mantenimiento con el fabricante el CABB podrá tener acceso a su web de soporte para entre otros:

- consulta de BBDD del equipamiento y licencias contratadas con las fechas de expiración
- posibilidad de apertura en directo como cliente de incidencias y/o RMAs con el fabricante
- posibilidad de descarga de software
- consulta sobre el estado de los casos abiertos por el integrador.

Como norma general y salvo que en la reunión de lanzamiento del proyecto especificada en el apartado 2.2 del presente documento no se especifique lo contrario:

- Para el caso de **nuevo equipamiento**, la activación de los mantenimientos y licenciamiento, salvo la debida justificación técnica o por petición expresa del CABB, debe coincidir con **fecha de puesta en producción** de los equipos en la red del CABB, siguiendo los plazos acordados en la reunión de lanzamiento del proyecto y acordes con lo presentado por el licitador en su oferta. La demora o incumplimiento de estos plazos supone la posibilidad de aplicar penalizaciones contempladas en el pliego administrativo del presente proyecto, pudiendo incluso implicar la rescisión del contrato
- En las **renovaciones** de mantenimiento y licenciamiento se considera un **plazo máximo** de **1 semana después de la firma de contrato** para que puedan estar activas en los equipos y siempre teniendo en cuenta los plazos de caducidad de los mantenimientos y licenciamientos de equipos en producción.
- Puede ser necesario, a petición del CABB, la presentación de la documentación o una notificación oficial por parte del fabricante que acredite el lanzamiento del pedido de compra de dicho mantenimiento y licenciamiento. La demora o incumplimiento de este plazo supone la posibilidad de aplicar penalizaciones contempladas en el pliego administrativo del presente proyecto, pudiendo incluso implicar la rescisión del contrato.

Completando lo mencionado previamente, como requerimientos generales el adjudicatario deberá cumplir con los siguientes:

- El periodo de garantía del nuevo equipamiento objeto de este expediente se extenderá durante toda la duración del contrato para el hardware y el software, a partir de la fecha de puesta en producción de los equipos.
- Se deberá dar soporte y mantenimiento a los equipos actuales por parte del integrador y fabricante en las mismas condiciones que el nuevo equipamiento a suministrar hasta que los equipos que los sustituyen estén plenamente operativos dando servicio en producción

De forma general, el mantenimiento abarca el soporte hardware y software, la renovación de licencias, así como la asistencia por parte de la empresa para la resolución de incidencias derivadas de averías, mal funcionamiento o vulnerabilidades desde la renovación del equipamiento ya instalado o finalizada la puesta en marcha en caso del nuevo equipamiento. La oferta, además, deberá incluir todas las licencias tanto hardware como software necesarias para el correcto funcionamiento de los equipos con todas las prestaciones solicitadas.

En los casos que así proceda, la empresa adjudicataria del contrato se encargará de realizar todas las gestiones para generar y administrar las RMAs con el fabricante, recogida del material, etc. Deberá hacerse cargo de todos los cargos que puedan generar sin coste alguno para el CABB. Esto incluye las gestiones necesarias para abrir, seguir casos, hacer pruebas con soporte, envío de información a soporte y elaborar informes de los casos abiertos con el fabricante.

Durante el periodo de tiempo que cubre el mantenimiento de la presente oferta, toda actualización software será responsabilidad de la empresa contratada sin gastos adicionales para CABB, independiente de si la actualización de versión comprende saltos de tipo “MAJOR” o “MINOR”, debido a los siguientes motivos:

- mal funcionamiento de los equipos derivado de la versión
- bugs de las versiones software actuales que afecten a la casuística particular del CABB
- vulnerabilidades de seguridad reconocidos por el fabricante en las versiones de producción, previo estudio de la criticidad de la vulnerabilidad y afección a la casuística particular del CABB
    - *En el caso de que la vulnerabilidad sea categorizada como crítica y/o afecte a la casuística particular del CABB de forma grave, se podrá solicitar la actualización de versión en un plazo no superior a 1 día*.
- próxima caducidad del software debido a que deja de ser soportado por el fabricante (EoS)

En caso de que dichas actualizaciones puedan interferir con el trabajo normal de los usuarios, se deberán de realizar fuera de la jornada laboral, pudiendo ser además requerimiento, la presencia física en la sede para una rápida intervención en caso de algún tipo de problema e independientemente de que el tipo de actualización sea referente a una versión y/o revisión mayor o menor de firmware y todo debe estar incluido en el contrato de mantenimiento y soporte de la empresa adjudicataria, sin que pueda implicar un

Así mismo, si la actualización de alguno de los equipos objeto del proyecto puede implicar, por compatibilidad entre versiones, la necesidad de actualizar otro equipamiento del CABB con el que estén relacionados (dichos equipos también deberán ser actualizado por el adjudicatario del pliego, sin que pueda suponer gastos adicionales para CABB.

Para finalizar es necesario tener en cuenta 3 aspectos fundamentales relacionados con el mantenimiento y que deben estar contemplados dentro del servicio que proporcionará la empresa licitadora:

2.5.1 Mantenimiento correctivo

Resuelve las incidencias o errores derivados del funcionamiento de los equipos o configuraciones. La forma de prestación del servicio será la siguiente:

- El personal del contratista recibirá especificaciones del error detalladas por parte de los técnicos del Consorcio o de empresas externas autorizadas por el CABB para dicha labor.
- Dicho personal efectuará las correcciones, gestiones con el fabricante y pruebas necesarias para resolver el problema.
- Finalmente documentará las modificaciones y comunicará la resolución de la incidencia y los cambios efectuados.

Este tipo de mantenimiento no será imputable a la bolsa de horas y debe estar contemplado en la oferta por parte del contratista.

2.5.2 Actualización de versión anual de los equipos

Con el objeto de mantener las versiones de los equipos a los que hace referencia la presente oferta actualizados desde el punto de vista de funcionalidades de seguridad y prestaciones, el CABB se reserva el derecho a solicitar, en la casuística que así proceda, una actualización anual de las versiones de los equipos consensuando dicha versión con la empresa contratista y fabricante.

Este tipo de actualización anual de versiones no implicará ningún sobrecosto para el CABB, ni será imputable a la bolsa de horas, debiendo estar contemplada en la oferta por parte del contratista como labores de mantenimiento.

2.5.3 Mantenimiento evolutivo o adaptativo

Surgirá a petición del CABB o de propuestas aportadas por la empresa contratista para mejorar o adaptar el sistema a nuevas situaciones. La forma de prestar el servicio será la siguiente:

- El Consorcio decidirá los cambios o mejoras a realizar determinando la prioridad de las ejecuciones.
- El personal del contratista ejecutará los trabajos.
- Finalmente documentará el trabajo y se lo comunicará y enviará al responsable del Consorcio. El contratista redactará las instrucciones de manejo.

Estos trabajos serán imputados de acuerdo con la bolsa de horas establecida del integrador

2.6 Servicio de asistencia técnica especializada

2.6.1 Fabricante

Por un lado, dada la casuística específica del proyecto y el cambio que supone para el CABB evolucionar desde una arquitectura de VPN tradicional a una arquitectura de ZTNA+SWG de red SASE, será necesario que la oferta del licitador cuente con un Servicio de Asistencia Técnica Especializada por parte de fabricante de un mínimo de 4 jornadas para, mediante su experiencia, abordar labores complejas del proyecto como pueden ser: diseño de la arquitectura en base a la casuística particular del CABB, recomendaciones de seguridad y buenas prácticas, seguimiento de una correcta implantación y migración por parte del integrador, solucionar posibles complicaciones y otras tareas complejas para las que se requiera su conocimiento y experiencia.

Por otro lado, dado que la tecnología SASE está en constante evolución y presenta múltiples funcionalidades y licenciamientos, el proyecto deberá incluir durante toda la duración del mismo asesoramiento y seguimiento

por parte del fabricante en aspectos como: correcta aplicación de funcionalidades contratadas, posibilidades y alternativas para el CABB de evolución en arquitecturas SASE, recomendaciones ….

2.6.2 Integrador

Se requiere un servicio Asistencia Técnica especializada de 25 horas por año de contrato para ejecutar tareas como la optimización de configuraciones, resolución de incidencias complejas, aplicación de nuevas funcionalidades y cualquier otra tarea que tenga relación con el objeto y equipos mencionados en el pliego con la posibilidad de ejecución en horario 24x7, dependiendo del tipo de tarea a ejecutar y si puede suponer corte de servicio.

El CABB podrá empezar a hacer uso de este servicio tras su validación final de la puesta en producción del presente proyecto, siempre que las tareas solicitadas queden debidamente justificadas como tareas fuera del servicio de mantenimiento y soporte contratado.

Dependiendo de las tareas a realizar, el CABB podrá solicitar que dichas tareas se realicen en remoto o si lo ve necesario, presencialmente en sus oficinas de Albia o en cualquier instalación del CABB a la que aplique la tarea a ejecutar.

En el caso de necesidad de que alguna tarea sea realizada presencialmente en alguna de las instalaciones del CABB, el integrador no podrá imputar al servicio de Bolsa de Horas ni los costes ni el tiempo de desplazamiento derivados del mismo.

Habitualmente este servicio se planificará con el adjudicatario con un mínimo de un día de antelación.

La forma habitual de prestar el servicio será la siguiente:

- El Consorcio decidirá los cambios o mejoras a realizar determinando la prioridad de las ejecuciones.
- El personal del contratista ejecutará los trabajos.
- Finalmente documentará el trabajo y se lo comunicará y enviará al responsable del Consorcio. En caso necesario redactará las instrucciones de manejo.

La solicitud del servicio se llevará a cabo por parte del CABB comunicando a la empresa contratista:

- Las nuevas necesidades
- Los cambios o modificaciones por realizar
- Los errores de las configuraciones

El personal responsable por parte del CABB planificará, de forma conjunta con el contratista, las fechas de inicio y fin y los recursos a aplicar a las tareas encomendadas.

El Consorcio suministrará al adjudicatario toda la documentación de la que disponga para el desarrollo del trabajo.

En todos los casos, será el personal responsable del CABB el interlocutor con los usuarios.

El contratista deberá entregar a los responsables de la Subdirección de Informática del CABB lo siguiente, en el caso de que así se requiera:

- Documentación de los procedimientos a seguir para obtener nuevas prestaciones o corrección de anomalías.
- Un informe diario breve de los trabajos realizados en la tarea en cuestión

- Documentación de las modificaciones realizadas y adaptar los manuales o procedimientos existentes del CABB en caso de que dicha modificación les afecte.
- Un informe mensual con información detallada de los trabajos realizados diariamente cuando proceda referentes a las tareas ejecutadas en el servicio de Bolsa de Horas.
- Un informe anual resumen de todas las tareas y estado del servicio.

2.7 Documentación

En general la documentación a entregar en la ejecución del proyecto cumplirá con lo siguiente:

- Documentación requerida por los servicios de PRL del CABB
- Planning detallado de las diferentes fases, tareas e hitos del proyecto, así como estimación de fechas de cada una de ellas.
- Inventario del nuevo equipamiento y licencias a instalar en formato especificado por el CABB. Identificación según el etiquetado proporcionado por CABB, será necesario entregar esta documentación en formato Excel específico que se indicará por el personal del CABB indicando además la fecha del fin del soporte de cada elemento, incluyendo licencias, transceivers, fuentes y otras características a especificar por el CABB según la casuística del proyecto.
- Documento de sugerencias, propuestas y mejoras de la arquitectura y configuración actual de los equipos.
- Planes detallados de alto y bajo nivel (HLD y LLD) de las diferentes fases a abordar en la migración, especificando especialmente en detalle la duración y acciones a realizar en las ventanas de corte necesarias en la migración.
- Plan de migración en el que se detallen los diferentes pasos a ejecutar y posibles cortes para la puesta en producción.
    - En dicho documento se debe detallar adecuadamente los diferentes pasos que se seguirán durante la puesta en producción y migración de la solución, haciendo especial hincapié en aquellos pasos que puedan suponer algún tipo de corte y su duración.
    - En aquellos casos que así proceda, será obligatoria la presentación de un documento por instalación y será necesaria su aprobación por parte del CABB antes de abordar la puesta en producción.
- Plan específico de pruebas y validación a completar con los valores obtenidos antes y después de la migración, detallando especialmente las pruebas de redundancia de la solución.
- Manuales de uso para el usuario final
- Documentos para la validación de la puesta producción entre los que debe estar presente:
    - Manuales para la apertura de incidencias con la empresa integradora con los diferentes métodos de contactos y formas de apertura de incidencias
    - Manuales para la apertura de incidencias con el fabricante con los diferentes métodos de contactos y formas de apertura de incidencias
    - Manuales con comandos de troubleshooting básicos para realizar futuro mantenimiento y configuración de los equipos.
    - Procedimiento de RMA de equipo a nivel Hardware, licencias y contratos de mantenimiento
    - Procedimiento de descarga de versiones, licencias en los equipos y procedimiento de actualización y backup para la casuística específica del CABB teniendo en cuenta los Sistemas centrales de recolección de logs y de gestión y administración.
    - Recomendaciones de mantenimiento, versiones del software instalado en los equipos, manuales y documentación relacionada con los procedimientos de soporte etc.

original de todo el software, programas y las licencias suministradas, justificante de abono y un manual de instalación de las mismas.

Y toda la documentación complementaria que el contratista considere necesaria para la administración y mantenimiento.

Toda esta documentación a realizar deberá contemplarse e incluirse en la realización de la oferta, no pudiéndose imputar estas tareas a la bolsa de horas. Así mismo, se deberá entregar en formato original de diseño y en formato PDF, de tal manera que ésta siempre pueda ser editada y/o modificada utilizando los correspondientes programas de edición.

Los documentos, tablas, cálculos, etc… se realizarán preferiblemente en formato DIN-A4. Se utilizará Microsoft Office como soporte informático.

Toda la documentación se presentará en castellano. Para los catálogos se admitirá el inglés.

Toda esta documentación se deberá elaborar siguiendo las especificaciones y los estándares entregados en las diferentes fases del proyecto.

Todos los programas y copias de seguridad a todos los efectos serán propiedad del CONSORCIO DE AGUAS.

NOTA: Toda la documentación realizada y aprobada en fase de ingeniería deberá ser actualizada con las modificaciones surgidas en puesta en marcha para la elaboración de la documentación "As built" a entregar y debe estar incluido dentro del alcance de documentación del proyecto.

2.8 Formación

La formación relativa al proyecto comprenderá 2 partes:

1- Transferencia de conocimiento sobre el proyecto al equipo técnico del CABB que se encargue de la explotación y mantenimiento de la solución compuesto por un total de hasta 5 personas del CABB y empresas colaboradoras externas.
   a. Se estima una duración aproximada de una jornada laboral con horario de 8:00 a 15:00
   b. El temario será acordado y validado previamente con el CABB y en función del grado del avance del proyecto se podrá solicitar que la formación sea proporcionada justo en la fase de migración. Entre otros aspectos se tratarán:
      i. Introducción a la nueva arquitectura y tecnología para la casuística del CABB
      ii. Detalle del proyecto ejecutado
      iii. Explotación
         1. Manejo de las diferentes herramientas
         2. Configuración de las acciones habituales (alta de usuarios, reglas…)
      iv. Mantenimiento
         1. Comandos y posibles fallos habituales
         2. Revisión de logs y alarmas
         3. Informes
2- Formación oficial de fabricante sobre la tecnología para un grupo de al menos 3 personas con las siguientes características:
   a. Duración aproximada de 3-4 jornadas
   b. Horario de 8:00-15:00
   c. El temario será acordado y validado previamente con el CABB, tratándose de dar especial relevancia a la parte de la tecnología que aplica al proyecto del CABB

2.9 Otras consideraciones

Todos los sistemas propuestos deberán poder integrarse y prestar servicio dentro de la actual arquitectura del CABB. Los elementos hardware ofrecidos deben ser totalmente compatibles con la arquitectura, hardware y software, del sistema de electrónica de red del CABB. Será responsabilidad del adjudicatario la ejecución de todas aquellas adaptaciones, configuraciones y parametrizaciones de productos necesarias para satisfacer dicho requerimiento.

Todo el equipamiento incluido en la oferta por parte del licitador debe ser perfectamente compatible entre sí y con el equipamiento disponible actualmente en las redes del CABB.

El proyecto se considera “llave en mano”, acometiendo el contratista todos los trabajos y suministros que sean necesarios para el correcto funcionamiento de los equipos con la configuración y programación necesarias.

El contratista deberá de presentar un planning detallado de la previsión en el desarrollo de los trabajos.

Los trabajos objeto del proyecto se han de realizar sin interferir con el trabajo normal de los usuarios, por lo tanto, todo trabajo que suponga un corte del servicio se deberá de realizar fuera de la jornada laboral.

La empresa adjudicataria deberá colaborar con el fabricante durante la instalación de la solución, para la realización de tareas conjuntas de análisis, diseño, instalación y configuración de la herramienta.

Todo equipamiento ofertado deberá ser nuevo y original del fabricante (tanto equipos activos como equipos pasivos tipo transceptores ópticos), siendo motivo de exclusión del concurso la inclusión de cualquier material no original del fabricante.

El CABB debe aparecer como propietario del equipamiento suministrado y debe constar como tal en las bases de datos del fabricante de dicho equipamiento.

En el caso de que alguno de los equipos (incluido ópticas, cables, memorias y demás componentes solicitados) tuviera anunciado el fin de soporte por parte del fabricante, el licitador deberá realizar su oferta incluyendo el equipamiento propuesto por el fabricante para su sustitución.

Todo el equipamiento solicitado se entregará con la última versión del sistema operativo recomendada por el fabricante en el momento del suministro y previamente aprobado por el CABB.

Cualquier componente, tanto hardware como software, no descrito en los diferentes apartados de este pliego, y que fueran necesarios para el cumplimiento de los diferentes requisitos funcionales, deberá ser incluido en la oferta.

Además de los suministros descritos, en los casos que proceda, se deberán de tener en cuenta el resto de pequeños suministros contemplados en el presupuesto (desmontajes, limpieza de locales, etc.)

Durante el periodo de tiempo que cubre el mantenimiento de la presente oferta, toda actualización software debido a motivos de mal funcionamiento, algún tipo de bug o vulnerabilidades de seguridad reconocidos por el fabricante en las versiones de producción, será responsabilidad de la empresa contratada sin gastos adicionales para CABB y en caso de que dichas actualizaciones puedan interferir con el trabajo normal de los usuarios, dichas actualizaciones se deberán de realizar fuera de la jornada laboral, siendo además requerimiento la presencia física en la sede para una rápida intervención en caso de algún tipo de problema.

3 RECEPCIÓN Y SEGUIMIENTO DE LAS INCIDENCIAS

El adjudicatario pondrá a disposición del CABB un teléfono único para toda la gestión de todas las incidencias reportadas, así como una cuenta de correo mediante los cuales poder abrir y realizar el seguimiento de las mismas.

También se indicará en la oferta la disponibilidad de realización y seguimiento de las incidencias mediante el acceso a la aplicación WEB de gestión de incidencias del licitante, describiendo brevemente dicha herramienta de incidencias.

Estas tres formas de apertura de incidencias podrán ser empleadas indistintamente por los responsables del CABB o empresas externas autorizadas por el CABB para dicha función.

Además, será necesario proporcionar a los responsables del Consorcio una forma de contacto directo (por correo electrónico y teléfono) con la persona o personas designadas como responsable del contrato de mantenimiento del equipamiento del CABB y del servicio de Bolsa de Horas para poder contactar en caso de algún tipo de urgencia crítica o de detectar desviaciones importantes en la resolución de incidencias.

Aunque actualmente no esté disponible, se podrá exigir en el futuro al adjudicatario el uso de la aplicación de incidencias del CABB/BBUP para la gestión y documentación de aquellas incidencias que estén relacionadas con el contrato, basado en el momento de la elaboración del pliego en JIRA software.

3.1 Gestión de incidencias

El siguiente apartado describe el método para la gestión de las incidencias recibidas y su tratamiento por parte del licitador con relación a todo lo que respecta al presente pliego con contrato de soporte durante la duración del mismo.

Las incidencias recibidas por el licitador se deberán consultar, en caso de duda, con el personal técnico del CABB para su categorización, atender según el tiempo estimado según los acuerdos de nivel de servicio, documentar y describir detalladamente las diferentes acciones realizadas y la solución final aportada por el licitador en toda su extensión rellenando los campos asociados en la aplicación de gestión de incidencias de forma que pueda ser consultadas por el personal del CABB u otros colaboradores de empresas externas asignadas por el CABB a labores de mantenimiento.

Las incidencias pueden ser abiertas por personal del del CABB u otros colaboradores de empresas externas asignadas por el CABB a labores de mantenimiento.

En caso de ser necesario, el técnico de la empresa licitadora al que se le asigne la incidencia deberá informar sobre la generación y el estado de la misma en cualquier momento, independientemente del horario y según los procedimientos acordados, al personal del CABB u otros colaboradores de empresas externas asignadas por el CABB a labores de mantenimiento que estén de guardia, notificándoles y comunicándoles con el nivel de detalle que se requiera, y realizar un posterior seguimiento de la evolución de la incidencia, anotando líneas de progreso y explicaciones sobre el detalle de la incidencia a medida que se van conociendo.

La explicación y líneas de progreso de la incidencia deberán ser técnicamente fundamentadas y reflejar fielmente lo indicado por el personal técnico del CABB u otros colaboradores de empresas externas asignadas por el CABB a labores de mantenimiento. Además, deberán estar correctamente redactadas, resultar de fácil comprensión y carecer de faltas de ortografía. Las siglas y elementos técnicos mencionados deben ser precisos y correctos.

La empresa licitadora mantendrá durante la fase de vigencia de la incidencia y hasta su cierre una comunicación fluida con el personal técnico del CABB u otros colaboradores de empresas externas asignadas por el CABB a labores de mantenimiento, ejerciendo de coordinador de la resolución y persiguiendo siempre la actuación óptima de las intervinientes y la máxima eficiencia en las actuaciones. Atenderá en todo momento a las instrucciones técnicas del CABB u otros colaboradores de empresas externas asignadas por el CABB a labores de mantenimiento, o del personal de guardia en horario no laboral, para asegurar que la evolución de la incidencia satisface sus indicaciones.

En el caso de incidencias críticas, la adjudicataria definirá, junto al CABB, un protocolo de notificación de incidencias críticas específico, en el que se debe comunicar de forma automática a responsables del CABB, determinadas incidencias con corte de servicio sobre un impacto importante que excedan de un determinado tiempo, así como hacer seguimiento y comunicar su resolución. La implantación de los mecanismos automáticos de este procedimiento, así como el seguimiento y su resolución, serán una de las funciones de la adjudicataria.

Una vez resuelta la incidencia, procederá a su cierre, cumplimentando la información adicional requerida, y confirmando dicho cierre con el personal técnico del CABB, pudiendo ser necesario, dependiendo del tipo de incidencia y las implicaciones que haya tenido en la red del CABB, la necesidad de presentar un informe en donde se detalle lo ocurrido, las acciones realizadas y medidas tomadas para solucionar el problema y evitar que se reproduzca en un futuro.

La empresa adjudicataria empleará para la gestión de las incidencias una aplicación WEB de gestión de incidencias propia, que deberá describir adecuadamente en su propuesta, en el apartado de medios materiales la propia aplicación y puede que sea necesaria, en un futuro, su integración con la herramienta interna de gestión de incidencias del Service Manager del CABB basada en JIRA Cloud. Se deberá permitir el acceso a los responsables técnicos del CABB u otros colaboradores de empresas externas asignadas por el CABB a labores de mantenimiento en los diferentes perfiles, de consulta o incluso generación, modificación y cierre de incidencias, según el modelo de relación acordado con la adjudicataria. Esta aplicación de gestión de incidencias deberá alimentar los informes entregados al CABB. El responsable del CABB deberá tener completa accesibilidad a los datos internos contenidos en la aplicación. Las licencias asociadas a esta nueva aplicación deberán ser suministradas al CABB y deberán poder ser utilizadas por ésta en el futuro sin costes adicionales posteriores.

Se estima que, como máximo, del personal interno del CABB u otros colaboradores de empresas externas asignadas por el CABB a labores de mantenimiento que deban tener acceso a la aplicación, 3 de ellos deberán tener perfiles operativos/administrativos, y se requerirán otros 2 perfiles consultivos. El coste de las licencias necesarias, para dichos accesos, si las hubiera, serán responsabilidad del adjudicatario y sin generar, por tanto, ningún sobrecosto para el CABB, debiendo estar contemplados en la oferta. La simultaneidad de accesos es baja. No obstante, se debe explicitar en la oferta las posibilidades de ampliación de personal con acceso a la herramienta y su coste económico, si lo tuviera.

El CABB podrá solicitar a la empresa adjudicataria la explotación de los datos de la aplicación de incidencias, para la preparación y entrega al CABB los informes que éste requiera. Estos informes tendrán una periodicidad trimestral y tendrán detalles de desglose de incidencias por día y mes, según tipos de incidencias, etc… También contendrán reportes de cumplimientos de los SLA del CABB, en función de los tiempos y número de incidencias de cada servicio. La cantidad de informes, su contenido y presentación podrán variar durante la prestación del servicio según las instrucciones del CABB dentro de un proceso de mejora continua.

3.2 Elaboración de informes de mantenimiento

El CABB podrá solicitar en todo momento a la empresa adjudicataria la elaboración de informes de seguimiento de servicio con, por lo menos, la periodicidad y detalle que se presentan a continuación:

- Informe **mensual** de tickets pendientes y su distribución por subsistema/servicio.
- Informe **trimestral** de tickets, tickets con corte, plazo medio de recuperación, tiempos de desplazamiento; todos ellos por subsistema.
- Informes **anuales** de cumplimiento de SLA del servicio prestado.
- Informes **trimestrales** y **anuales** de cumplimiento de SLAs del servicio.

El CABB podrá requerir también la elaboración de informes periódicos de estadísticas del servicio, tanto en lo referente a calidad en la recepción de incidencias como en su resolución: incluyendo número de incidencias por instalación, descripción, fecha, etc… Por ejemplo, y entre otros posibles, se incluirá un listado con las incidencias generadas (descripción de la incidencia, estado, fecha de creación y resumen), otro listado con las incidencias generadas por cada instalación (descripción de la incidencia, estado, fecha de creación y resumen), y una tabla resumen con el número total de incidencias por instalación para el período acordado.

Adicionalmente se elaborarán los informes de SLA relativos al servicio prestado por la adjudicataria al CABB, según los compromisos del contrato.

4 CARACTERISTICAS DEL SERVICIO

4.1 Horario del servicio, lugar de trabajo y desplazamientos

El horario del servicio para las acciones que no suponen corte del servicio se realizará en horas de oficina preferiblemente. Cualquier ampliación de este horario deberá ser acordada con la Dirección del Proyecto.

Se considera horario de oficina de LUNES-JUEVES 7:30-17:30h y VIERNES 7:30-15:00h

Los trabajos que supongan corte del servicio se realizarán preferentemente fuera del horario laboral. En ningún caso esto supondrá sobrecosto alguno para el CABB.

Los tiempos de respuesta y resolución solicitados en el presente "Pliego de Prescripciones Técnicas" para los elementos incluyen la realización de los trabajos durante las 24 horas de los 365 días del año.

En función de los requerimientos de las tareas a realizar los recursos necesarios para prestar el servicio requerido se ubicarán en las sedes específicas del CABB o en remoto desde las oficinas del contratista, informando al CABB. No obstante, el CABB puede requerir, según su criterio en relación a las labores a realizar, la presencia de los técnicos en sus instalaciones en cualquier momento, sin que ello suponga ningún incremento de precio por viajes, desplazamientos, dietas, etc… con lo que en los precios unitarios presentados en la oferta del licitador deberán estar contemplados todos los gastos adicionales que dichos desplazamientos pudieran ocasionar. Por lo tanto, será cuenta del adjudicatario los desplazamientos, gastos de manutención y todos los medios humanos.

4.2 Acuerdo de nivel de servicio (ANS/SLA)

4.2.1 Bolsa de horas

Se considera horario laboral de LUNES-JUEVES 7:30-17:30h y VIERNES 7:30-15:00h.

Para la solicitud de los trabajos a realizar en Bolsa de Horas se notificará con una **antelación mínima** de:

- UN DÍA de antelación para actuaciones clasificadas como URGENTES
- UNA SEMANA de antelación para actuaciones clasificadas como NO URGENTES

El tiempo de resolución estimado para cada trabajo solicitado por Bolsa de Horas no se puede estimar ya que dependerá de la naturaleza del mismo. No obstante, sí se estima conveniente que para los casos de extrema urgencia que no serán habituales, pero supongan una situación crítica que impliquen cortes no cubiertos por los correspondientes contratos de soporte y mantenimiento, especificar un tiempo de resolución inferior a 4 horas.

4.2.2 Mantenimiento y soporte

Para la atención de las averías de los elementos a mantener, dependiendo de la incidencia y a decisión del CABB, la forma de actuación por parte de los técnicos de la empresa licitadora deberá ser on-site, es decir, todos los trabajos se realizarán in situ en cualquiera de los centros e instalaciones del CABB o en remoto, en función de la tarea a realizar y consensuado con el CABB.

Los trabajos objeto del proyecto se han de realizar sin interferir con el trabajo normal de los usuarios, por lo tanto, todo trabajo que suponga un corte del servicio se deberá de realizar fuera de la jornada laboral.

- Tiempo de respuesta. Se establece en 1 hora para incidencias críticas y 1 día para incidencias no críticas, siendo decisión final del CABB la asignación de la criticidad o no de la incidencia. El tiempo de respuesta es el comprendido entre la notificación emitida por Consorcio de Aguas hasta el inicio de la intervención por parte del técnico de mantenimiento.
- Tiempo de resolución. Se establece un tiempo máximo de resolución de 4 horas los 365 días del año para las incidencias críticas y 2-3 días para incidencias no críticas. El tiempo de resolución será el comprendido desde la notificación del aviso a la empresa adjudicataria hasta el momento de su resolución u operatividad del elemento averiado.

El nivel de cumplimiento global debe ser igual o superior al 85 % del volumen de incidencias comunicadas por Consorcio de Aguas y cerradas en el mes evaluado.

Con el fin de garantizar una respuesta y agilidad en el servicio a incluir, la empresa licitadora deberá de garantizar proporcionar respuesta según el SLA acordado, esto es, 24x7x4 y el personal técnico adscrito a esta licitación deberá de estar asignado a un centro de trabajo que cumpla los SLAs acordados.

La demora o incumplimiento de alguno de alguno de los puntos expuestos supone la posibilidad de aplicar penalizaciones contempladas en el pliego administrativo del presente proyecto, pudiendo incluso implicar la rescisión del contrato.

4.3 Control y seguimiento del servicio

Se creará un Comité de seguimiento del Servicio formado por una o dos personas del Consorcio, pertenecientes a la Subdirección de Informática u otros colaboradores de empresas externas asignadas por el CABB a labores de mantenimiento y los responsables designados por el contratista. Este Comité de seguimiento resolverá los conflictos que pudieran suscitarse y tendrán las reuniones necesarias para conseguir un servicio satisfactorio.

En caso de ser necesario, para agilizar las labores de control y de seguimiento se confeccionarán unos informes, redactados con la periodicidad que se determine, que serán analizados y aprobados por el Comité de seguimiento. El documento deberá recoger también las incidencias y su resolución.

El CABB podrá solicitar programar reuniones in situ en las oficinas del CABB/BBUP o en remoto vía Microsoft Teams o similar, con la periodicidad que el CABB determine y en las que se tratarán los siguientes aspectos a nivel general:

- Cumplimiento de objetivos e indicadores del nivel de calidad del servicio
- Incidencias del servicio
- Avance de las mejoras
- Planificación de los trabajos

En lo que se refiere a las labores exclusivas relacionadas con la ejecución del proyecto se realizará una reunión inicial al comienzo del proyecto (kick-off) con el fin de realizar un análisis de la situación actual y en la que el contratista proporcionará un planning detallado con las diferentes tareas, hitos, fases y fechas de cumplimiento del proyecto y un posible enfoque de mejora del diseño actual. Posteriormente se planificarán reuniones de seguimiento, por defecto con periodicidad semanal hasta la finalización del despliegue. El contratista deberá entregar un acta de la reunión en formato Word, OneNote u otro formato, según se acuerde entre el contratista y los responsables del contrato del CABB al inicio del contrato. El tiempo empleado en las reuniones de seguimiento, así como para la elaboración de las actas de reunión deben contemplarse a la hora de la redacción de la oferta puesto que no se deberán imputar a la bolsa de horas.

4.4 Aportaciones del Consorcio

El Consorcio suministrará al adjudicatario toda la documentación de la que disponga para el desarrollo del trabajo.

En todos los casos, será el personal responsable del Consorcio el interlocutor con los usuarios.

4.5 Aportaciones del contratista

Deberá entregar a los responsables de la Subdirección de Informática del Consorcio lo siguiente:

- Documentación, procedimientos, esquemas, diagramas… derivados del proyecto o sistemas del CABB modificados e implicados en el mismo en los formatos indicados por el CABB.
- Tramitación de documentación y permisos solicitados por el departamento de PRL del CABB.
- Documentación de las modificaciones realizadas para la resolución de las incidencias peticiones de Bolsas de Horas con los cambios efectuados.
- Un informe mensual con información detallada de los trabajos realizados diariamente cuando proceda (Bolsas de Horas o peticiones específicas del CABB)
- Un informe diario breve de los trabajos realizados durante la asistencia en labores de mantenimiento o Bolsa de Horas por peticiones específicas del CABB
- Un informe trimestral de los accesos de los usuarios durante dicho período cuando proceda.

4.6 Forma de comunicación-contacto

El contratista comunicará por escrito la designación de las persona o personas de su organización, encargadas de ejercer las facultades de dirección, organización y disciplinarias en lo referente a los técnicos que prestan los servicios contratados, tanto a nivel de:

- labores de ejecución del proyecto
- labores de mantenimiento y soporte
- labores relacionadas con Bolsa de Horas.

Será necesario proporcionar a los responsables del Consorcio una forma de contacto directo con dicha persona o personas (por correo electrónico y teléfono) para poder contactar en caso de algún tipo de urgencia crítica o en caso de detectar desviaciones importantes en la ejecución del proyecto, resolución de incidencias de soporte y solicitud de los diferentes niveles de tareas de las Bolsas de Horas

El adjudicatario pondrá a disposición de los usuarios para la recepción y seguimiento de las incidencias un teléfono único para toda la gestión de todas las Incidencias reportadas, así como una cuenta de correo mediante los cuales poder abrir y realizar el seguimiento de las incidencias.

De cara a la forma habitual de contacto para las labores de ejecución del proyecto, el CABB formará un equipo de trabajo compuesto por personal del CABB u otros colaboradores de empresas externas asignadas por el CABB que se comunicarán con el equipo técnico asignado por el adjudicatario del proyecto, pudiendo establecer diferentes métodos de contacto para el seguimiento y ejecución de las diferentes tareas del proyecto y que se acordará en la reunión inicial (kick-off) como son: contacto telefónico, correo electrónico, reuniones presenciales y/o telemáticas, aplicaciones colaborativas como Microsoft Teams…

En lo que respecta al contacto habitual para las labores de mantenimiento y soporte, la empresa adjudicataria proporcionará al CABB los procedimientos habituales de apertura de incidencias de mantenimiento tanto por personal del CABB u otros colaboradores de empresas externas asignadas por el CABB en el que, entre otros aspectos, como mínimo se especifique de forma clara y concisa:

- Credenciales y procedimiento de apertura incidencias 24x7 mediante la aplicación WEB de gestión de incidencias del adjudicatario
- Credenciales y procedimiento de apertura incidencias 8x5 mediante la aplicación WEB de gestión de incidencias del adjudicatario
- Teléfono de contacto y procedimiento de apertura incidencias 24x7 mediante llamada telefónica
- Teléfono de contacto y procedimiento de apertura incidencias 8x5 mediante llamada telefónica
- Correo electrónico y procedimiento de apertura incidencias 24x7 por correo electrónico
- Correo electrónico y procedimiento de apertura incidencias 8x5 por correo electrónico
- Otros procedimientos de aperturas de incidencias

Por último, de cara al contacto habitual del servicio de Bolsa de Horas se acordará con el adjudicatario la forma de contacto para la solicitud de este servicio, siendo lo habitual su solicitud mediante correo electrónico o aplicación WEB específica diferente a la que recoge las peticiones de mantenimiento y soporte.

5 COMPROMISO DE CONFIDENCIALIDAD Y CIBERSEGURIDAD

El adjudicatario queda expresamente obligado a mantener indefinidamente, absoluta confidencialidad y reserva sobre cualquier dato que pudiera conocer con ocasión del cumplimiento del contrato, especialmente los de carácter personal, que no podrá copiar o utilizar con fin distinto al que figura en este pliego, ni tampoco ceder a otros ni siquiera a efectos de conservación.

El licitador que se proponga como adjudicatario aportará una memoria descriptiva de las medidas que adoptarán para asegurar la disponibilidad, confidencialidad e integridad de los datos manejados y de la documentación facilitada. Asimismo, deberá incluir en dicha memoria la designación de la persona o personas que, sin perjuicio de la responsabilidad propia de la empresa, estarán autorizadas para las relaciones con el CABB a efectos del uso correcto del material y de la información a manejar. Esta obligación de guardar la confidencialidad subsistirá, aunque se extinga el contrato, hasta que dicha información pierda tal carácter, o bien si se produce la debida autorización por parte del CABB.

De conformidad con la Disposición Adicional vigésima quinta de la Ley 9/2017, 8 de noviembre, de Contratos del Sector Público, el adjudicatario quedará obligado al cumplimiento de lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal y garantía de los derechos digitales, y en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, debiendo suscribirse el correspondiente contrato previsto en el artículo 28 del Reglamento 2016/679 dentro del mes siguiente a la formalización del contrato.

Respecto a la ciberseguridad, el objetivo pretendido es dar cumplimiento a la normativa y legislación aplicable al CABB. Entre otras, son de aplicación: Esquema Nacional de Seguridad (ENS) con mínimos de nivel MEDIO, Reglamento General Europeo de Protección de Datos (RGPD), Real Decreto de seguridad de las redes y sistemas de información (Directiva NIS), Ley de Protección de infraestructuras Críticas (PIC). De modo general, se establecen requisitos que debe satisfacer el contratista, aplicando las medidas de seguridad adecuadas para cumplir la legislación a la que está obligada a CABB, así como la Política de Seguridad de la Información y normativas vigentes en la entidad. En el caso de incumplimiento de cualquiera de las obligaciones incluidas en la presente cláusula, el adjudicatario será responsable del importe íntegro de cualquier sanción que, en materia de protección de los sistemas de información, pudiera ser impuesta a CABB, así como de la totalidad de los gastos, daños y perjuicios que sufra CABB como consecuencia de dicho incumplimiento.

6 ESPECIFICACIONES TÉCNICAS DE LA SOLUCIÓN

6.1 Especificaciones generales

La solución SASE propuesta debe ofrecer las siguientes prestaciones generales:

- Plataforma única desde la que se entregan todos los casos de uso SASE
- Gestión conjunta de plataforma desde una sola consola.
- Alta disponibilidad y auto-escalado incluidos por defecto
- Infraestructura y direccionamiento IP (Ingress/Egress) únicos y dedicados
- Aproximación Zero Trust Network Access (ZTNA) completa
- Seguridad avanzada e integral para todos los casos de uso cubiertos por una solución SASE.
- Visibilidad y control de TODO el tráfico de TODAS las aplicaciones
- Todas las funcionalidades de seguridad aplicadas a todo el tráfico todo el tiempo, tanto en la navegación a internet como en el acceso a aplicaciones privadas.
- Capacidad de gestión remota de los usuarios móviles
- Capacidad multitenant
- Mejorar la experiencia de usuario independientemente de su localización.
- Incluir un mínimo de 366 días de retención de logs en caliente de todo el tráfico procesado.
- Capacidad de realizar log forwarding desde el entorno SASE a un elemento SIEM y/o syslog externo.
- Múltiples capacidades de autenticación para la identificación de usuario como son SAML, Kerberos, LDAP, RADIUS, TACACS+, MFA, Explicit proxy vía SAML, Local Database.

6.2 Especificaciones particulares

Complementando con lo indicado en el apartado 2.3 del presente documento, la solución SASE debe prestar las siguientes funcionalidades:

6.2.1 Prestaciones particulares a nivel de gestión

- Ofrecer una consola única de gestión desde la que configurar, monitorizar y mantener los casos de uso SASE principales, incluyendo expresamente Proxy en la nube, SWG, FWaaS, ZTNA, SD-WAN, CASB en línea, CASB API, SSPM, DLP y gestión de la experiencia de usuario (DEM, Digital Experience Management)
- Consolidar los logs en un punto común, al menos para las funcionalidades de navegación en internet y acceso a aplicaciones privadas. En ambos casos la solución debe correlacionar automáticamente los logs relativos a una misma sesión, es decir, si para una sesión el tráfico pasa por el servicio de proxy o de firewall, por inspección de URL y por inspección de amenazas, tales logs deben correlacionarse automáticamente para simplificar el análisis de un posible problema o incidente de seguridad
- Permitir configurar distintos tipos de autenticación para diferentes propósitos, estableciendo un orden de prioridad entre ellos, de tal forma que se compruebe cada tipo de autenticación en función de su orden de prioridad hasta que uno de ellos autentique correctamente al usuario.
- Tener la capacidad de evaluar la configuración e identificar áreas de mejora, detectar objetos y/o reglas configuradas, pero sin uso o identificar la presencia de reglas demasiado permisivas.
- Disponer de la capacidad de gestión unificada (de forma nativa desde la nube) de la solución.
- Aplicar las mismas políticas avanzadas de seguridad a la nube similares a las que se pueden aplicar en los firewalls de nueva generación on-premise.
- Incluir de forma integrada la capacidad de visibilidad de experiencia de usuario a nivel de aplicación común para equipos on-premises y usuarios móviles. Mismo punto de gestión y troubleshooting

6.2.2 Prestaciones particulares a nivel de arquitectura del servicio en la nube

- Garantizar una disponibilidad del 99,999% de servicio mediante SLAs.
- Medir SLAs del servicio sobre disponibilidad, procesamiento de la seguridad (incluyendo SSL decrypt y análisis de motores antimalware) y a nivel de aplicación SaaS de terceros.
- Limitar a un máximo 10 milisegundos la latencia para descifrado, inspección de seguridad y cifrado del tráfico, tanto para la navegación segura como para el acceso a aplicaciones privadas.
- Ofrecer la mayor seguridad y evitar fluctuaciones de rendimiento, el tránsito entre regiones/zonas/PoPs de la solución propuesta no debe ser a través de internet si no a través de redes privadas. De tal forma que, si un usuario se conecta al PoP1 para acceder a un recurso que está conectado al PoP2, el tráfico entre PoP1 y PoP2 no pase por internet.
- Poseer la infraestructura de seguridad 100% desplegada sobre varios de los principales proveedores de nube pública reconocidos en el mercado.
- Proporcionar una infraestructura de seguridad en la nube **dedicada para el CABB**, sin posibilidad de compartir el plano de datos con otros clientes.
- Tener la capacidad de despliegue de la infraestructura de seguridad en varios proveedores de nube pública en paralelo para obtener redundancia en caso de fallo de una región cloud de un proveedor.
- Poder dividir el licenciamiento entre varios tenant de tal forma que sea posible crear varios tenant gestionados desde una consola común pero independientes en el plano de datos:
    - con infraestructura independiente y dedicada por tenant
    - con IPs de servicios independientes y dedicadas por tenant
- Disponer de la capacidad de integrar y activar en el mismo agente de puesto de usuario y en los appliances de seguridad on-premises el software necesario para disponer del módulo de visibilidad y troubleshooting avanzado a nivel de aplicación que permita la monitorización transparente de aplicaciones SaaS y aplicaciones on-premises.

- Contar con prestaciones de auto-escalado para el tráfico de usuarios móviles, de tal forma que, si los recursos en la nube superan ciertos umbrales, automáticamente se desplieguen más recursos para absorber incrementos de demanda de tráfico.
    - Esto debe ocurrir sin coste adicional, sin configuraciones adicionales y sin intervención de operadores.
- Ofrecer alta disponibilidad por defecto, tanto para el acceso de usuarios móviles como desde oficinas, de tal forma que, en caso de fallo del punto activo de conexión, automáticamente se active uno de backup.
    - Esto debe ocurrir sin coste adicional, sin configuraciones adicionales y sin intervención de operadores
- Permitir el uso de aplicaciones en las que la comunicación se inicia desde el CPD hacia el cliente, por ejemplo, aplicaciones de help-desk remoto, FTP activo o Voz sobre IP
- Permitir el uso de aplicaciones por parte de los usuarios en movilidad que usen protocolos como UDP, ICMP, Multicast para acceder a servicios alojados en los CPD privados.

6.2.3 Prestaciones particulares a nivel del servicio de seguridad en la nube

- Estar certificada al menos por:
    - ENS nivel Medio
    - ISO27001
    - ISO27017
    - ISO27018
- Incluir la funcionalidad de FWaaS (Servicio de Firewall en la nube o similar) con, como mínimo, funcionalidades de:
    - Deep Packet Inspection (DPI)
    - Identificación de aplicaciones
    - Definición de políticas en base a aplicaciones y no solamente en base a direcciones IP, puertos y protocolos
    - Seguridad DNS
    - Capacidades de IPS/IDS
    - Capacidades de antivirus, antimalware y Sandbox para todo el tráfico, no solamente para el tráfico web
- Ofrecer las funcionalidades de seguridad basadas en soluciones propias, no en acuerdos de reventa de terceras soluciones (acuerdos OEM) ni en soluciones open source
- Poseer la capacidad de detectar la aplicación a nivel 7, independientemente del puerto de nivel 4 por el que la aplicación se comunica, tanto en la navegación, en acceso mediante proxy, como en el acceso a aplicaciones privadas
- Poder forzar un cambio dinámico de políticas aplicadas si, una vez establecida la sesión, se modifica la postura de seguridad del dispositivo. Este cambio dinámico de políticas debe estar disponible tanto para la navegación a internet como para el acceso a aplicaciones privadas
- Tener la capacidad de detectar y detener el robo y envío de credenciales corporativas (usuarios y password de la red corporativa) hacia las webs que se visitan, de forma que se pueda advertir, bloquear o permitir dicho envío de credenciales en función de las categorías de web visitadas
- Implementar, de forma unificada, tanto la securización del tráfico hacia Internet (tráfico web y no web) como la securización del tráfico hacia aplicaciones internas (tráfico web y no web).
- Proporcionar el servicio de seguridad en la nube, tanto para la securización de la navegación como para el acceso a aplicaciones privadas, con las siguientes funcionalidades mínimas :

- Firewall Nivel 7 a nivel de aplicación
  - SSL Decryption
  - Antimalware eficiente frente a ataques de SQL injection y C2 Cobalt Strike
  - Antispyware
  - Antivirus
  - IPS
  - URL Filtering con capacidad de analizar el contenido de las respuestas web en tiempo real y no basarse solo en bases de datos de categorizaciones.
  - DNS Security con las siguientes protecciones y características:
    - Known malicious domains
    - High-risk domains
    - DGA domains
    - DNS tunneling
    - Fast-flux domains
    - DNS rebinding attacks
    - Dictionary DGA
    - Dangling DNS attacks
    - NSNX denial of Service
    - Prediction detection of new domains
    - Ultra-slow DNS tunneling
  - Sandboxing capaz de inspeccionar tanto archivos descargados (inbound) como archivos subidos (outbound), ya sean servidores internos o sitios públicos en internet y con, como mínimo, los siguientes métodos de detección de amenazas (tanto para Windows, linux, Android y MacOS):
    - Dynamic Analysis
    - Static Analysis
    - Machine Learning
    - Custom Hypervisor
    - Bare Metal Analysis
    - Dynamic Unpacking
    - Network Pattern Matching
    - Recursive analysis
    - Multi-Vector Recursive Analysis
    - Inline Machine Learning detection
    - Hornet Engine Static Analysis
- Tener la posibilidad de proporcionar servicio de seguridad en la nube avanzado, tanto para la securización de la navegación como para el acceso a aplicaciones privadas, previa adquisición de su licencia específica, con las siguientes funcionalidades:
  - CASB inline
  - CASB API
  - DLP como
  - IoT Security
- Implementar técnicas de Machine Learning de forma automática para la mejora continua de los rangos de detección y prevención frente a amenazas conocidas, sus variantes y amenazas nuevas para las funcionalidades de antimalware, URL Filtering, Sandboxing.
- Aplicar las mismas políticas avanzadas de seguridad a TODO el tráfico de TODAS las aplicaciones

- Poder

proteger el tráfico web y aplicar servicios de seguridad avanzada a nivel 7 sin arquitectura proxy en la nube.

- Poseer la capacidad de modificación de las decisiones iniciales de confianza en base a la detección de amenazas de seguridad.
- Disponer de una seguridad inline consistente, teniendo la opción de aplicar los mismos controles de seguridad mencionados anteriormente tanto al tráfico destinado hacia Internet/Aplicaciones SaaS como al tráfico hacia aplicaciones corporativas tradicionales situadas en entornos privados (DataCenter/ IaaS)
- Crear automáticamente firmas para nuevos malware detectados y distribuirlas a los componentes de la solución SASE en menos de 10 segundos

6.2.4 Prestaciones particulares a nivel del servicio de ZTNA

- Poder aplicar las mismas capacidades de seguridad para protección del tráfico de navegación y para protección del acceso a aplicaciones o recursos privados.
- Soportar capacidades de DLP (previa adquisición de licenciamiento correspondiente) en el acceso a aplicaciones privadas para usuarios móviles o remotos (conectados con agente), para usuarios que acceden directamente desde oficinas conectadas con la nube SSE (sin agente) y para usuarios móviles o remotos que acceden sin agente.
- No limitar el acceso a un número determinado de aplicaciones privadas, debe permitirse el acceso a tantas aplicaciones privadas como se estimen oportunas en cada momento.
- No hacer NAT del tráfico de los usuarios que acceden a las aplicaciones o recursos privados, de tal forma que estos vean la IP origen de los usuarios, para una mejor visibilidad y trazabilidad
- Poder proporcionar capacidades de aceleración de aplicaciones de tal forma que, para usuarios remotos o usuarios conectados en sedes remotas, el acceso a las aplicaciones corporativas a través de la nube y con todas las capacidades de seguridad habilitadas, sea más rápido que el acceso directo a través de internet
- Aplicar políticas ZTNA en base a:
    - Autenticación del usuario
    - Autenticación del dispositivo
    - Postura de seguridad del dispositivo
    - Detección de amenazas de seguridad

6.2.5 Prestaciones particulares a nivel del servicio de conectividad de usuario

1- Para las conexiones <u>CON agente software</u>
    a. Detección fiable de usuario en situación de dentro o fuera de la red interna del CABB mediante diferentes métodos y con la opción de desactivar el envío de tráfico hacia la nube cuando se detecte que el usuario esté conectado a la red interna del CABB.
    b. Amplio soporte de sistemas operativos (incluido Windows, Linux y MAC)
    c. Capacidad de securizar el acceso a Internet y a las aplicaciones privadas que se encuentran en los centros de datos o sedes remotas
    d. Posibilidad de acceso a la solución mediante acceso proxy sin necesidad de instalación de agente para los usuarios corporativos conectados a la red interna del CABB
    e. Capacidad de publicación de aplicaciones internas desde IP públicas dedicadas en el servicio cloud ofertado
2- Para las conexiones <u>SIN agente software</u>
    a. Opción de acceso al usuario final mediante:

   i. navegador empresarial específico para la solución SASE con funcionalidades de seguridad avanzadas
   ii. navegadores webs habituales más empleados (Google Chrome, Mozilla Firefox, Microsoft Edge, Safari…)

b. Integración de forma nativa del navegador empresarial en la solución de SASE, con capacidad de acceso a aplicaciones tanto públicas como privadas sin necesidad de usar o instalar herramientas adicionales.
c. Capacidad de gestionar tanto tráfico web como protocolos RDP/SSH directamente desde el navegador y con todas las capacidades de seguridad intrínsecas.
d. Configuración de políticas de seguridad con capacidades Zero Trust a través del contexto de:
   i. Usuario: usuario, grupo de usuario, direccionamiento IP o localización
   ii. Postura del equipo: información (tipo, modelo, fabricante), si es gestionado o no, información del OS (versión, screen lock, integridad, contraseña, etc.)
   iii. Aplicación: URL, aplicación específica, categoría, tipo de cuenta o tenant SaaS
   iv. Direccional: políticas basadas en grupos de aplicaciones con riesgos "similares". Por ejemplo, habilitando solo la transferencia de ficheros y el "copia/pega" entre aplicaciones dentro del mismo grupo.
e. Características y funcionalidades de seguridad avanzadas para el caso de acceso mediante navegador empresarial específico para la solución SASE:
   i. Capacidad de aplicar políticas de seguridad basadas en la postura de seguridad del equipo, incluyendo:
      1. Versión del OS (windows y MacOS)
      2. Número de serie
      3. Certificado cliente
      4. Cifrado del sistema de ficheros
      5. Bloqueo de pantalla
      6. Protección del endpoint
      7. Tipo de equipo (Desktop, Laptop, VM, etc.)
      8. Protección del OS por password (especificando la complejidad de la misma)
      9. Fabricante del equipo(Microsoft, Dell, Apple, etc.), especificando el modelo
      10. Integridad del sistema
      11. Verificación de "normal OS boot mode"
      12. Gestión del equipo (especificando Microsoft Intune, Azure AD, Jamf, Active Directory)
      13. Conexión remota activa
      14. Llaves de registro
   ii. No deberá pedir permisos de administrador para poder ser instalado
   iii. Soportar todas las extensiones de Chrome de manera predeterminada.
   iv. Capacidad de aislar su propio ambiente de trabajo del equipo, habilitando a los usuarios a trabajar de manera segura en equipos que pudiesen estar comprometidos, a través de los siguientes mecanismos:
      1. Añadiendo una capa de seguridad a través del cifrado de los recursos del navegador en el disco y la memoria (credenciales, cookies, tokens, etc.), incluyendo protección contra keyloggers
      2. Protegiendo contra alteraciones con múltiples técnicas de chequeo de integridad

3. Aplicando múltiples mecanismos de seguridad contra ataques de redes man in the middle
4. Protegiendo la sesión del navegador ya sea bloqueando cuando la sesión queda en "idle", o limpiando los datos del navegador de forma periódica
5. Evaluando la postura de seguridad del equipo como mínimo cada 90 segundos para asegurar que se está ejecutando en un ambiente seguro.

v. Disponer de capacidades de protección web embebidas, así como protección contra extensiones maliciosas.

vi. Capacidades de seguridad que deberá incluir el navegador:
1. Protección anti-malware para la transmisión de ficheros
2. Protección anti-phishing con URL filtering
3. Protección contra componentes vulnerables comunes de un navegador, como pueden ser JavaScript JIT, WebRTC, etc.
4. Protección contra extensiones maliciosas (permitir o no permitir, monitorización de riesgo, metadata y popularidad, y mayor control granular)
5. Funcionalidad de safesearch para filtrar contenido inapropiado de buscadores como Google, Bing, DuckDuckGo y Youtube.
6. Control sobre el ciclo de vida del "patching" del motor Chromium usado por el navegador.

vii. Aportar información de seguridad para análisis, investigación de eventos, análisis forense y búsqueda de amenazas:
1. Recopilando registros de auditoría de cualquier acción web (navegación, login, carga/descarga de ficheros, eventos de clipboard, imprimir, pantallazo, etc.)
2. Eventos enriquecidos con metadata como el hash del fichero, path, URL de origen/destino, etc.
3. Posibilidad de anonimizar los datos para mantener la privacidad del usuario sin recopilar información personal
4. Posibilidad de capturar la grabación de las acciones del usuario en la aplicación web (antes y después del evento para análisis forense)
5. Posibilidad de monitorizar los equipos en uso, metadata, su postura presente y pasada, extensiones instaladas, etc.
6. Posibilidad de monitorizar las aplicaciones usadas, acceso, violaciones de información, tamaño del fichero, tanto las.

viii. Disponer de un motor de seguridad capaz de crear políticas de acceso, datos e identidad a escala.

ix. Ofrecer múltiples tipos de controles granulares, como, por ejemplo:
1. Bloqueo de sitios web o categorías
2. Permitir o no permitir el "login" de dominios de correo específicos en aplicaciones determinadas
3. Control sobre la carga/descarga de ficheros, basado en el tipo, tamaño, hash o etiqueta MIP del fichero.
4. Bloqueo de la acción de copiar/pegar de información entre aplicaciones y fuera del navegador
5. Bloqueo de la acción de imprimir o compartir pantalla, así como pantallazos sobre aplicaciones web
6. Marcas de agua sobre sitios web

7. Enmascaramiento de la información sensible en los sitios web, ya sea en ficheros o evitando que los usuarios escriban esta información directamente
8. Control sobre el uso de cámara/micrófono.

x. Proporcionar un robusto control de identidad a través de los siguientes mecanismos:
   1. Gestión de contraseñas: Securizando de forma nativa el acceso a sitios web a través del sistema de gestión de contraseñas embebido en el navegador
   2. Multi factor Authentication (MFA): Posibilidad de solicitar MFA como un pincode o passkey en cualquier acción del usuario sobre un sitio web, como navegación, carga/descarga de fichero, copiar/pegar, etc.
   3. Permisos Just In Time (JIT): Aplicando mensajes personalizados a los usuarios ante acciones en el navegador, y permitiendo el acceso a los usuarios ya sea especificando una razón, o pidiendo la razón del usuario para tener el acceso y la aprobación por parte del administrador.

6.2.6 Prestaciones particulares a nivel de fabricante de la solución

- Servicio de soporte directo de fabricante que ofrezca un acompañamiento desde la implantación del despliegue hasta su operación y mejora evolutiva durante la duración del contrato
- Reuniones periódicas con fabricante para poder revisar la evolución de la solución SASE su adopción asegurando:
  - El despliegue sigue su planificación reduciendo las desviaciones
  - Se adoptan las funcionalidades proporcionadas por la solución para maximizar el rendimiento y la seguridad
  - Asistencia en la incorporación de nuevos casos de uso fuera del alcance inicial del proyecto
  - Escalado de caso y orquestación de los equipos de fabricante para minimizar los tiempos de resolución de incidencias o desviaciones de despliegue.
- Soporte a integraciones de la plataforma con terceros y recomendaciones de configuración
- Análisis proactivo de estado de salud y postura de la solución con tal de asegurar la mejor experiencia de usuario y maximizar la seguridad

7 TABLA RESUMEN

A continuación, a modo de referencia, se muestra una tabla con los equipos, servicios y licencias a instalar y mantener durante la duración del contrato que se deberá presentar en el Pliego de Condiciones Técnicas ofertados por el licitador SIN incluir precios:

ID	REFERENCIA	DESCRIPCIÓN	CANT.
1		Licencias para 200 usuarios con funcionalidades ZTNA *(especificar en la tabla correcta referencia y descripción según fabricante)*	200
2		Licencias para 200 usuarios con funcionalidades SWG *(especificar en la tabla correcta referencia y descripción según fabricante)*	200
3		Licenciamiento específico de fabricante necesario para dar servicio a lo especificado en el pliego *(especificar en la tabla correcta referencia y descripción según fabricante)*	-
4		Soporte 24x7x4 fabricante anual durante toda la duración del contrato	1

ID	REFERENCIA	DESCRIPCIÓN	CANT.
5		Soporte integrador 24x7x4 anual durante toda la duración del contrato	1
6		Servicio de Ingeniería para migración, puesta en marcha y documentación de la solución	1
7		Servicio de Ingeniería para Integración de la solución con los sistemas de monitorización del CABB	1
8		Servicio de Asistencia técnica especializada de fabricante para la implantación de la arquitectura	1
9		Servicio de Asistencia técnica especializada de fabricante de seguimiento tecnológico posterior a la implantación y puesta en marcha	1
10		Servicio de Bolsa de Horas de Asistencia técnica especializada de integrador en las tecnologías del proyecto 25 horas/año	1
11		Formación	1