Financiado por la Unión Europea

GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSICIÓN ECOLÓGICA Y EL RETO DEMOGRÁFICO

Plan de Recuperación, Transformación y Resiliencia

Bilbao Bizkaia Ur Partzuergoa
Consorcio de Aguas Bilbao Bizkaia

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES

SUMINISTRO, INSTALACION Y MANTENIMIENTO DEL SISTEMA DE SECURIZACIÓN PERIMETRAL DE LAS SEDES PERIFÉRICAS DEL CABB 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 "DENOMINADA TRANSICIÓN DIGITAL EN EL SECTOR DEL AGUA (ENFORCEMENT DIGITAL MEDIOAMBIENTAL)".

Índice

1 OBJETO DEL PROYECTO.

El objeto principal de este pliego es el suministro, instalación y mantenimiento del sistema de securización perimetral de las sedes periféricas de la red del Consorcio de Aguas, en adelante CABB, con el objetivo de remplazar los sistemas de securización perimetral actuales, los cuales dejarán de estar soportados por el fabricante según su anuncio de fin de soporte de los mismos, en las siguientes ubicaciones:

1. ETAP IPARRAGUIRRE
2. OFICINAS BARAKALDO
3. OFICINAS GERNIKA
4. OFICINAS XUPERA
5. PRESA ORDUNTE
6. PRESA UNDURRAGA
7. ETAP BASATXU
8. ETAP GARAIZAR
9. ETAP GARTXETA
10. ETAP GOROZIKA
11. ETAP JARRALTA
12. ETAP OLETA
13. ETAP SALINILLAS
14. ETAP SAN CRISTOBAL
15. ETAP SAN MIGUEL
16. ETAP SAN SALVADOR
17. ETAP SOLLANO
18. OFICINAS BERMEO
19. OFICINAS BILBAO

El principal objetivo es renovar, modernizar y mejorar las funcionalidades, prestaciones y capacidades de la infraestructura tecnológica actual que se encargan de securizar las comunicaciones del CABB en sus sedes periféricas.

El presente pliego comprende todas las tareas para el suministro, documentación, configuración, instalación, migración, puesta en marcha, mantenimiento y posterior asistencia técnica tras la puesta en producción de los nuevos equipos de securización.

Como características generales, los nuevos equipos de securización perimetral suministrados deben ser appliance físico y poseer funcionalidades y capacidades superiores a los actualmente instalados en el CABB.

Los nuevos equipos también deben ser compatibles con sus actuales sistemas de centrales de recolección de logs del CABB (FortiAnalyzer 3000G) y sistemas centrales de gestión de configuraciones (FortiManager VM64). En caso de existencia de algún tipo de incompatibilidad o necesidad de ampliación HW o SW, se deberá dejar perfectamente especificado en la oferta y será obligación del licitador, sin ningún coste extra para el CABB:

- En caso de la necesidad de adquisición de nuevos sistemas de centrales de recolección de logs del CABB y/o de nuevos sistemas centrales de gestión de configuraciones será obligación del licitador la de suministrar, instalar, configurar y mantener el nuevo equipamiento necesario con características, funcionalidades, prestaciones, capacidades, licenciamiento y configuraciones similares o superiores a los actuales (FortiAnalyzer 3000G y FortiManager VM64), pero nunca inferiores durante el tiempo de duración del pliego.

- En caso de la necesidad de actualizar las versiones o ampliar las licencias actuales de los sistemas de centrales de recolección de logs del CABB y/o de los sistemas centrales de gestión de configuraciones actuales, el licitador deberá tener en cuenta en el presente pliego la actualización de versión o ampliación de licencia necesaria para ambos equipos (FortiAnalyzer 3000G y FortiManager VM64), así como la posible actualización de versión que otros sistemas de securización perimetral del CABB también administrados por ambos sistemas puedan necesitar para seguir siendo compatibles con estos últimos, siguiendo las especificaciones y requerimientos del CABB para su actualización (aproximadamente otros 45 equipos de securización perimetral modelos 61F y Rugged-60F).

El proyecto como mínimo debe incluir las siguientes fases, tareas e hitos:

1. Planificación de reuniones de seguimiento y planning detallado de las diferentes fases, tareas e hitos del proyecto, así como estimación de fechas de cada una de ellas.

2. Replanteo de las instalaciones y análisis de la configuración del equipamiento actual de los sistemas de securización perimetral y otro equipamiento que pueda estar relacionado con el objetivo principal del proyecto como puede ser:
    a. Sistemas centrales de recolección de logs, eventos e informes de los sistemas de securización perimetral (FortiAnalyzer 3000)
    b. Sistemas centrales de gestión y administración (Fortimanager VM)
    c. Otros sistemas de securización perimetral también gestionados por los dos sistemas anteriores
    d. Sistema de monitorización interno y externo (NOC)
    e. Otros sistemas del CABB relacionados

3. Documentación detallada y especificada en el apartado 2.7 del presente documento.

4. Suministro, instalación y configuración de equipos de securización de capa 7 con el diseño y características acordados en la fase previa de documentación aprobada.

5. Integración de los equipos de securización de capa 7 en la infraestructura actual de monitorización y gestión interna del CABB tanto para la administración centralizada de los mismos como para la gestión de sus logs y elaboración de informes de tráfico, así como otras herramientas internas del CABB.

6. Servicio de mantenimiento de proveedor en 24x7x4 durante toda la duración del contrato.

7. Servicio de mantenimiento de fabricante 24x7 con RMA NBD durante toda la duración del contrato con 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 como como cliente de incidencias y/o RMAs, así como descarga de software y posibilidad de consulta sobre el estado de los casos abiertos por el integrador.

8. Bolsa de asistencia técnica especializada de 50 horas por año de contrato para la optimización de las 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

9. Servicio de monitorización (NOC) 24x7x4 del equipamiento al que hace referencia el presente pliego. Dicha monitorización se realizará en dependencias externas a CABB y mediante herramientas de gestión basadas en SNMP o syslog propias de la empresa adjudicataria pero que serán accesibles por CABB para poder consultar. Ante la activación de una alarma con motivo de dicha monitorización se activará un procedimiento de actuación redactado por la empresa adjudicataria con las indicaciones y validación por parte del CABB para la resolución de la alarma en remoto o presencialmente en la sede, activando el soporte de integrador o fabricante 24x7x4 de forma automática en caso de que fuera necesario para la resolución de la alarma detectada.

10. Todo el etiquetado, pasacables, paneles y cableado (UTP y fibra óptica) necesario para abordar los trabajos.

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 consideración 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 de 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, 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, mantenimiento y posterior asistencia técnica de sistemas de securización para las sedes que conciernen a dicho proyecto. Para ello, se ha considerado que el sistema en la mayoría de las instalaciones debe constar de al menos:

- Un solo equipo o bien una pareja en alta disponibilidad de cortafuegos de NGFW con software, licenciamiento y las características mínimas especificadas en el apartado 6 del presente documento
- Etiquetado, pasacables, paneles y cableado (UTP y fibra óptica), etc.. necesarios para la correcta instalación de todos los elementos en sus respectivas instalaciones.

El contratista deberá tener en cuenta que cada instalación tiene unas particularidades diferentes y deberá contemplar la adecuación de las mismas, dentro del alcance del 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 Replanteo de instalaciones

El presente pliego incluye programar una primera visita inicial o replanteo a cada una de las instalaciones del proyecto en compañía de personal del CABB o de una empresa intermediaria designada por el CABB en un plazo máximo de **siete (7) días laborales** después de la firma de contrato para:

- Conocer el estado de la instalación.
- Documentar el estado actual y compararlo con la información disponible de la instalación.
- Revisar el estado del cableado, tomas de red, canalizaciones de la instalación y otra información de interés.
- Escoger la ubicación donde se va a instalar el nuevo equipamiento en la sede (tanto el posible provisional como el final)
- Hacer una estimación del material y cableado necesario para la realización de los trabajos en función de la ubicación escogida.
- Obtener la información necesaria para la elaboración de la documentación:

Una vez realizada esta primera visita, el adjudicatario en un plazo máximo de **siete (7) días laborales** y tras la confirmación del CABB el contratista realizará el pedido del equipamiento y material necesario para abordar el proyecto.

En caso de que los plazos de entrega del material solicitado se demoren durante varios meses puede que sea necesaria una segunda visita o replanteo a las instalaciones antes de abordar la ejecución del proyecto para, entre otros:

- Comprobar posibles cambios en las instalaciones que puedan afectar al proyecto (cableado, tomas …)
- Ajustar el pedido del material a los cambios observados en esta segunda visita
- Modificar la documentación realizada a la nueva situación de la instalación

2.2 Suministro

El suministro comprende la entrega de todo el material necesario para que la instalación quede en funcionamiento de acuerdo con este PPTP.

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

Asimismo, el equipamiento debe entregarse con la imagen y las versiones del resto de equipos del CABB, indicadas en el presente Pliego o las que se indiquen en el momento de la entrega del material por parte del personal responsable del contrato del CABB y recomendadas por el fabricante. No obstante, en caso de que en el momento de la implantación se detecte por necesidades de funcionalidades o seguridad la actualización a una versión superior, el licitador será encargado de la actualización tanto de los equipos suministrados como de los equipos en producción, sin sobrecosto alguno para el CABB. También se debe tener en cuenta en la oferta la actualización del parque existente.

Por norma general, se considera 1 semana después de la firma de contrato o de la realización de los replanteos en los proyectos que así lo solicite el CABB, como el plazo máximo para la realización del pedido de compra del nuevo equipamiento al fabricante. Será obligatorio, en caso de solicitud expresa por parte del CABB, la presentación en dicho plazo de la documentación o una notificación oficial por parte del fabricante que acredite el lanzamiento del pedido de compra.

El plazo máximo de entrega del material en condiciones de mercado normales debe ser de 4 semanas a partir de la firma del contrato o de la fecha validada por parte del CABB tras la reunión inicial de lanzamiento del proyecto y/o del resultado obtenido tras la realización de los replanteos en los proyectos que así lo solicite el CABB, 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.

Como se ha mencionado previamente todo el equipamiento ofertado debe ser appliance físico, excepto lo expresamente indicado en el pliego. 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.

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

El presente proyecto debe incluir el servicio de Asistencia Técnica especializada necesaria para implementar las funcionalidades requeridas en el pliego.

2.3.1 Migración de los equipos de seguridad perimetral actuales al nuevo equipamiento suministrado

Se deberá contemplar todas las adaptaciones y cambios de configuración necesarios derivados de la instalación de los nuevos equipos objeto del pliego que puedan generar en otros firewalls, switches, equipos de monitorización, equipos de elaboración de informes, equipos que registran eventos y syslog, reglas de firewalls, controladoras inalámbricas, backup centralizado de configuraciones y copias de seguridad, etc… actualmente en producción en la red del CABB. Así como cualquier otro elemento de la red necesario para el sistema quede funcionando plenamente y cumpla los requisitos solicitados en el presente pliego.

Se deberá realizar la configuración de los equipos nuevos, a fin de que tengan a su entrega la misma imagen y versión de firmware que el resto del parque existente a petición del responsable del CABB o bien, que se solicite que todo el equipamiento solicitado se entregará con la última versión del sistema operativo recomendada por el fabricante en el momento del suministro o bien de la instalación y previamente aprobado por el CABB.

Se deberá realizar la configuración de las copias de seguridad de los equipos suministrados con frecuencia diaria en la en la herramienta del CABB para dicho fin.

El suministrador del equipo deberá realizar todas las cambios y configuraciones requeridas por el CABB para un correcto funcionamiento, hasta tener la arquitectura requerida en el proyecto. Así mismo, se valorarán todas las mejoras de configuración y funcionalidades que el licitador proponga por las nuevas prestaciones disponibles en el nuevo equipamiento adquirido o las nuevas versiones de software y licencias disponibles.

Deberá estar considerada en esta asistencia técnica la formación o transferencia de conocimiento que puedan implicar los trabajos realizados a los técnicos del Consorcio o de empresas externas autorizadas por el CABB.

2.3.2 Bolsa de Horas

Se requiere un servicio Asistencia Técnica especializada de 50 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 equipamiento objeto 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 Consorcio 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 Consorcio 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 Consorcio el interlocutor con los usuarios.

El contratista deberá entregar a los responsables de la Subdirección de Informática del Consorcio lo siguiente:

- 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.

2.4 Instalación de equipamiento

Se precisa la instalación y configuración del equipamiento ofertado y las pruebas necesarias para su puesta en funcionamiento.

Los equipos de securización deberán instalarse y configurarse para trabajar bien como equipo único, bien en alta disponibilidad (HA) en modo Activo- Pasivo. Específicamente, se deberán proporcionar los servicios de instalación y puesta en marcha, incluyendo todas las pruebas y soporte in situ necesarios para asegurar el completo y correcto funcionamiento de los equipos.

El hardware objeto de esta adquisición tendrá que ser configurado e instalado por la empresa adjudicataria, además de realizar las conexiones de cableado, todo ello según normas que establezca la Subdirección de Informática del CABB.

Se deberá asegurar la no interrupción del servicio, por lo que las intervenciones, cambios de configuración o puestas en marcha que puedan suponer corte de servicio se realizarán en las fechas y horarios autorizados por el CABB para ello (fines de semana inclusive).

La instalación inicial del nuevo equipamiento será in situ y consistirá en la manipulación física del mismo, conexionado y su configuración software de forma que el equipo quede perfectamente instalado y operativo de acuerdo con las indicaciones del personal del CABB.

Una vez finalizada la instalación, la empresa adjudicataria deberá etiquetar los equipos según normas que facilitará la Subdirección de Informática del CABB, para su posterior inventariado, así como todo el cableado relacionado con los nuevos equipos.

La empresa adjudicataria antes de proceder a la instalación deberá entregar un planning detallado de trabajos que deberá ser aprobado por el personal responsable del contrato del CABB.

2.5 Mantenimiento y licenciamiento

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

- Resolución de averías insitu o en remoto hardware o software en 24 horas cualquier día del año (24x7) por parte del integrador para toda la duración del contrato.
- Servicio de mantenimiento hardware o software 8x5 del fabricante de los equipos 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

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 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

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.

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 3 días*.
- 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, siendo 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 (FortiAnalyzer, Fortimanager…) 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 una actualización anual MAJOR o MINOR de las versiones de los equipos consensuando dicha versión con la empresa contratista.

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 aprobará 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.

2.6 Servicio de monitorización

2.6.1 Servicio de monitorización y gestión interna

Será también labor del licitador la inclusión de todo el nuevo equipamiento adquirido en el presente pliego en las diferentes herramientas y servicios de monitorización y gestión interna del CABB, según proceda:

- FortiAnalyzer
  - Recepción centralizada de logs
  - Generación de eventos de alarmas
    - Adecuación de todos los eventos de alarmas actuales al nuevo equipamiento y versión software de los equipos objetos del pliego
  - Generación de informes customizados periódicos basados en SQL
    - Adecuación de todos los informes actuales al nuevo equipamiento y versión software de los equipos objetos del pliego
- FortiManager
  - Gestión centralizada de configuraciones
  - Script automatizado para backup de configuraciones
  - Otros scripts para carga de configuraciones de políticas y objetos
- Intermapper
  - Gestión interna de monitorización mediante SNMP versión 2c y 3 del nuevo equipamiento

    - Generación nuevas sondas customizadas basada en SNMP para monitorización del nuevo equipamiento y entrega de documentación relacionada
- Otros
    - Posible adaptación de otras herramientas y aplicaciones de monitorización y gestión interna del CABB como servidor Netflow, Syslog, Ansible (con scripts basados en Python) …

2.6.2 Servicio de monitorización externa (NOC)

Servicio de monitorización continua del nuevo equipamiento al que se hace referencia en el presente pliego, mediante una herramienta de gestión basada en SNMP o similar en dependencias externas a CABB con el objetivo de detectar proactivamente fallos en los mismos y actuar en base a un procedimiento predefinido de manera autónoma.

Este servicio de monitorización externa (NOC) propuesto en la oferta debe ejecutarse en modalidad 24x7 durante todo el periodo de ejecución del contrato

Dicha monitorización tiene como objetivo principal la de realizar de forma proactiva labores de mantenimiento y soporte siguiendo unos diagramas de flujo y procedimientos de actuación que elaborará la empresa licitadora respetando las indicaciones del CABB/BBUP.

Los equipos actuales ya están siendo monitorizados mediante este procedimiento, siendo necesario que el servicio de monitorización externa (NOC) cumpla con unos requisitos iguales o superiores a los actuales, entre los que destacan:

- La herramienta de monitorización se tiene que ubicar en las instalaciones de la empresa integradora y conectar de forma segura con el CABB mediante un túnel IPSEC o similar.
- La herramienta de monitorización empleará un protocolo de gestión seguro como SNMP versión 3 o similar para la monitorización de la mayoría del equipamiento a excepción del que no sea compatible, en ese caso se utilizará el protocolo SNMP versión 2c o similar.
- Se deberá parametrizar las consultas SNMP que la herramienta realice hacia los diferentes equipos a monitorizar en función de la capacidad de las líneas del CABB para que dichas consultas no penalicen el funcionamiento habitual de las sedes y otros tiempos, a nivel general se considerarán los siguientes, aunque puede que sea necesario modificar en alguna sede a petición del CABB/BBUP y en función de las cargas y líneas de cada sede. A continuación, se proponen unos valores iniciales que puede ser modificados durante la ejecución del pliego:
    - Tiempo entre consultas en caso de que la respuesta a la misma sea correcta: 5 minutos
    - Tiempo entre consultas en caso de una primera respuesta en fallo: 2 minutos
    - Número de respuestas fallidas consecutivas antes de generar la correspondiente alarma: 5 (10 minutos)
    - Tiempo de espera del servicio del NOC desde que se genera una alarma hasta actuar según procedimientos definidos ante posible fallo puntual recuperable de forma automática:30 minutos
- La herramienta de monitorización se basará en una solución software basado en NAGIOS o similar.
- Se proporcionará al CABB/BBUP acceso en modo lectura a un dashboard de la herramienta de monitorización en la que se muestren los equipos monitorizados, sus variables y las alarmas activas de cada momento.
- En la herramienta de monitorización se visualizará en formato gráfico las diferentes variables mostrando un histórico de sus valores a lo largo del tiempo.

- Se valorará la posibilidad de que el dashboard de la herramienta de monitorización muestre también de forma gráfica las instalaciones a modo de mapa con las diferentes ubicaciones y equipos en cada una de las mismas.
- Aunque actualmente no esté disponible, se podrá exigir en el futuro al adjudicatario su integración con la aplicación de incidencias del CABB/BBUP, basada en el momento de la elaboración del pliego en JIRA software. De forma que las incidencias generadas por el servicio de monitorización del NOC queden también reflejadas en la aplicación de incidencias propia del CABB/BBUP.

La finalidad de dicha herramienta de monitorización es analizar el estado de los equipos en las instalaciones, así como analizar el estado del servicio en la que se encuentran los equipos instalados buscando:

- Identificar riesgos potenciales y cuellos de botella.
- Identificar eventos críticos tales como desconexiones, excesos de errores en los puertos, consumos de memoria, etc.
- Generar alarmas definidas con el CABB tales como cambios de configuraciones, acceso a un dispositivo, etc.
- Generar informes detallados que permitan a los responsables del CABB conocer la situación y participar en las acciones de análisis o corrección necesarias.
- Elaborar y ejecutar procedimientos de actuación ante la recepción de posibles alarmas detectadas por los sistemas de monitorización siempre consensuados con el CABB.
- Una vez definidos los procedimientos finales será necesario repasarlos y adecuarlos a posibles cambios trasladados por el CABB con una periodicidad mínima anual.

Previamente a la puesta en marcha habrá que determinar la relación de equipos y variables que han de ser especialmente monitorizados y realizando una propuesta y ajustes de configuración oportunos en los mismos. En principio, para cada equipamiento de seguridad perimetral al que se hace referencia en el pliego se estima monitorizar:

- Conectividad vía ICMP
- Estado HA
- Estado de memoria
- Estado de CPU
- Estado de Fuentes
- Estado de Ventiladores y Temperatura
- Número de conexiones concurrentes
- Estado BGP
- Número de rutas BGP aprendidas
- Estado de interfaces y/o agregados
- Ancho de Banda de interfaces y/o agregados

Será responsabilidad de la empresa adjudicataria del contrato, en colaboración con los responsables del CABB, la definición de los diagramas de flujos y procedimientos de actuación contando siempre con las necesidades y consideraciones propuestas por el CABB para su elaboración. También se deben realizar aquellas funciones básicas de operación que el CABB considere apropiadas y podrá solicitar su repaso o modificación en cualquier momento de la duración del contrato del presente pliego con el objeto de corrección de fallos en el mismo o proponer mejoras, incluyendo la modificación de los procedimientos y diagramas de flujos.

El servicio incluye la monitorización continua remota de las alarmas de red en las herramientas específicas que se designe desde la localización remota para la monitorización (Nagios o similar). La detección de un evento o alarma de red deberá derivar en la apertura proactiva de una incidencia y su gestión posterior de acuerdo con el procedimiento de actuación acordado.

2.6.2.1 Informes del servicio de monitorización externa (NOC)

El CABB podrá solicitar a la empresa adjudicataria la elaboración de informes con periodicidad **trimestral y anual** con estadísticas obtenidas de la herramienta de monitorización en el que se muestre una evolución a lo largo del tiempo del uso de los equipos en los que se debe incluir: memoria, CPU, BW de interfaces… incluyendo conclusiones de la evolución.

También se podrá solicitar 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.

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.
- Fotos actuales de la instalación, alrededores de los racks donde se instalen los equipos de securización, su interior y exterior
- Documentación según indicaciones del CABB para describir el acceso a las diferentes ubicaciones en las que se aloja el equipamiento objeto del contrato.
- 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
- 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 por instalación en el que se detallen los diferentes pasos a ejecutar y posibles cortes para la puesta en producción de cada una de las instalaciones objeto del proyecto.
    - En dicho documento se debe detallar adecuadamente los diferentes pasos que se seguirán durante la puesta en producción de la solución para cada instalación, haciendo especial hincapié en aquellos pasos que puedan suponer algún tipo de corte y su duración.
    - 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 para cada sede a completar con los valores obtenidos antes y después de la migración.

- Documentos para la validación de la puesta producción entre los que debe estar presente:
    - Fotos finales de la instalación, de los alrededores de los racks donde se instalen los equipos de securización, su interior y exterior.
    - Resultado de los planes de pruebas realizados en taller (pruebas FAT), donde corresponda, y en la sede durante la migración
    - Nuevos esquemas y documentación o actualización de los esquemas y documentación actuales del CABB en relación a todo los que el proyecto haya modificado directa o indirectamente en la red y sistemas del CABB.
    - Certificaciones del cableado y reflectometrías
        - En los casos en los que sea necesario el despliegue de fibra óptica en las instalaciones, se deberá entregar planos o mapas donde queden marcados los recorridos de la fibra en formato digital
    - 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, backup y restauración 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.
    - Documentación original de todo el software, programas y las licencias suministradas, justificante de abono y un manual de instalación de las mismas.
    - Documentación final del proyecto As Built

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.

La documentación generada se entregará tanto en papel como en soporte informático (1 copia en papel y otra en soporte informático).

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 Compatibilidad con la arquitectura del CABB

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.

2.9 Otras consideraciones

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, 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 relación con las incidencias derivadas del servicio de monitorización externa (NOC) según se defina en el procedimiento de actuación ante los diferentes eventos de alarmas acordados, tal y como de detalla en el apartado 2.6.2 del presente documento, deberán ser atendidas como incidencia, con una clasificación que los distinga. Asimismo, según se defina en el procedimiento acordado, el licitador, de manera proactiva y ante la recepción de las alarmas, generará incidencias de motu proprio y notificará de las mismas al personal del CABB u otros colaboradores de empresas externas asignadas por el CABB a labores de mantenimiento, ejecutando las tareas definidas para su resolución de forma autónoma o consultando con un técnico del CABB u otros colaboradores de empresas externas asignadas por el CABB a labores de mantenimiento, dependiendo de cómo se dicte en el procedimiento acordado en el servicio.

Además, 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/BBUP 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

La empresa adjudicataria elaborará los informes acordados en la definición inicial del modelo de servicio. Estos informes contendrán 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.

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.

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. Dichas actas de seguimiento deberán entregarse en el plazo no superior a 48h desde que se haya llevado a cabo la reunión de seguimiento. 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.

Además de las actas anteriormente mencionadas, los responsables del CABB si así lo consideran, podrán exigir al contratista la utilización de las herramientas del CABB, JIRA Service Manager, para el seguimiento de la planificación y los hitos del proyecto, para la gestión de todo el ciclo de vida del proyecto; siendo este requisito tenido en cuenta y contemplado en la elaboración de la oferta.

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 DEL NUEVO EQUIPAMIENTO

A continuación, se indican los requisitos mínimos a cumplir para todo el equipamiento del sistema de securización.

6.1 Sistemas de securización perimetral sedes periféricas

Como se ha indicado anteriormente, el proyecto consiste principalmente en el suministro de un sistema de securización compuesto principalmente por los equipos firewalls, uno o dos para cada centro; en el caso de ser dos se instalarán en clúster sustituyendo a los actuales. El presupuesto contemplará todos los trabajos previamente descritos en el presente pliego de forma que el sistema deberá cumplir con todas las funcionalidades requeridas y reemplazar y cumplir mayores funciones que las que realizan los equipos actuales.

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., especialmente con los equipos actuales para la gestión centralizada de las configuraciones y de logs.

6.1.1 Características generales mínimas necesarias

No se admitirán propuestas de equipamiento de menores características, funcionalidades y prestaciones de los que se equipos que se citan a continuación:

- Fortigate 71G o similar

Se debe considerar que los nuevos equipos sean capaces de funcionar teniendo todas las funcionalidades, licencias y soporte habilitadas durante toda la vida del contrato, sin verse afectado el rendimiento de los equipos de manera que pueda verse mermada la calidad del servicio (CPU <20% y memoria <40%) deben disponer de disco duro interno SSD cada firewall con capacidad mínima por disco de 64 GB que permita almacenar localmente los registros de logs en los propios equipos ante una posible caída de la conexión contra el sistema de registro centralizado de logs actual (FortiAnalyzer 3000G).

Por un lado, todo el equipamiento incluido en la oferta por parte del licitador debe ser perfectamente compatible entre sí y con los actuales sistemas de centrales de recolección de logs del CABB (FortiAnalyzer 3000G), con acceso por interfaz web y por CLI, a donde los equipos puedan enviar todos sus logs de tráfico en tiempo real y ser almacenados por un periodo mínimo de entre 3-6 meses para su posterior exportación a un servidor externo. Así mismo, será necesario que dichos sistemas centrales de recolección de logs puedan realizar informes personalizados basados en SQL y enviar alarmas por correo ante la recepción de cierto tipo de eventos Por otro lado, todo el equipamiento incluido en la oferta por parte del licitador también debe también ser compatible con los sistemas centrales de gestión de configuraciones centrales del CABB (FortiManager VM64) con acceso por interfaz web y por CLI, que permita la distribución simultánea de políticas a diferentes equipos y la creación de una base de datos de objetos común para todos los dispositivos administrados.

En caso de existencia de algún tipo de incompatibilidad o necesidad de ampliación HW o SW, se deberá dejar perfectamente especificado en la oferta y será obligación del licitador, sin ningún coste extra para el CABB:

- En caso de la necesidad de adquisición de nuevos sistemas de centrales de recolección de logs del CABB y/o de nuevos sistemas centrales de gestión de configuraciones será obligación del licitador la de suministrar, instalar, configurar y mantener el nuevo equipamiento necesario con características, funcionalidades, prestaciones, capacidades, licenciamiento y configuraciones similares o superiores a los actuales (FortiAnalyzer 3000G y FortiManager VM64), pero nunca inferiores durante el tiempo de duración del pliego.
- En caso de la necesidad de actualizar las versiones o ampliar las licencias actuales de los sistemas de centrales de recolección de logs del CABB y/o de los sistemas centrales de gestión de configuraciones actuales, el licitador deberá tener en cuenta en el presente pliego la actualización de versión o ampliación de licencia necesaria para ambos equipos (FortiAnalyzer 3000G y FortiManager VM64), así como la posible actualización de versión que otros sistemas de securización perimetral del CABB también administrados por ambos sistemas puedan necesitar para seguir siendo compatibles con estos últimos, siguiendo las especificaciones y requerimientos del CABB para su actualización (aproximadamente otros 45 equipos de securización perimetral modelos 61F y Rugged-60F).

Por último, todos los equipos suministrados deben proporcionar la funcionalidad de SDWAN sin necesidad de adquirir ninguna licencia adicional.

6.1.2 Especificaciones mínimas necesarias hardware

El equipamiento ofertado para su instalación en las sedes periféricas debe soportar como mínimo, las siguientes especificaciones hardware en condiciones óptimas:

- Hasta 1,4 Millones de conexiones concurrentes TCP
- Hasta 100.000 nuevas conexiones TCP por segundo
- Throughput IPv4 de hasta 10 Gbps sin ninguna funcionalidad capa 7 activada
- Throughput de hasta 2,5 Gbps con funcionalidades IPS y logging activados
- Throughput de hasta 1,5 Gbps con funcionalidades IPS, Control de Apps y logging activados
- Throughput de hasta 1,3 Gbps con funcionalidades NGFW capa 7 e inspección SSL de tráfico activadas
- Latencia de hasta 2,46 µs
- Hasta 5.000 políticas de seguridad configurables
- Hasta 10 FWs virtuales configurables por defecto sin licenciamiento adicional
- Hasta 10 puertos GigabitEthernet RJ45
- Hasta 1 disco duro SSD de 64GB
- Cables de alimentación para schucko o PDU según corresponda

Como referencia de características mínimas, para orientación de los ofertantes, se han considerado los equipos de la casa Fortinet. (modelo FG-71G) o similar.

6.1.3 Especificaciones mínimas necesarias software y licencias

Se requiere que los equipos a instalar tengan, como mínimo, una serie de funcionalidades y licencias durante toda la duración del contrato para las mismas:

- Control de aplicaciones
- IPS
- Antivirus
- Threat protection
- IP reputation & antibotnet security
- Sandbox cloud
- Doble factor de autenticación integrado en la misma plataforma y del mismo fabricante
- Comprobación de firmas de Antivirus en tiempo real contra una base de datos de inteligencia global del fabricante, sin esperar a recibir el paquete de actualización de firmas
- Capacidad para eliminar contenidos dinámicos de un documento para poder analizarlo entregando al usuario un primer archivo sano, sin contenido dinámico.
- Posibilidad de configuración de routing dinámico, en especial BGP y OSPF con las distintas opciones de filtrado de rutas que permiten ambos protocolos
- La solución debe proveerse en alta disponibilidad física.
- Control de la navegación Web por categorías de URL
- Control DLP de descarga/subida de archivos
- Inspección SSL del tráfico
- Identificación/navegación por identificación de usuario/grupo de usuarios
- Identificación en equipo de multiusuario
- Traffic shapping
- Control horario para aplicación de políticas
- Integración con Active Directory
- Modelo de licenciamiento no basado en el número de usuarios. No limitación de usuarios debido a licenciamiento
- Visualización de número de usos y cantidad de tráfico de cada regla. Así como de la última vez que se ha utilizado

- Activación y desactivación automática de las reglas por fecha y hora
- Reparto de carga dinámico de conexiones TCP entre diferentes servidores. Balanceo de carga entre servidores internos con chequeo de estado de estos y aplicación de algoritmos de balanceo avanzados:
  - Source IP Hash
  - Round Robin
  - Weighted Round Robin
  - First Alive o Least RTT
  - Least Session
- Posibilidad de realizar balanceo de tráfico entre las líneas de salida del cortafuegos en base a distintos algoritmos
- El sistema debe ser capaz de proporcionar redundancia de enlaces WAN monitorizando el estado de las líneas
- Los equipos deben disponer de al menos 6 dominios virtuales incluidos en el cortafuegos
- Arquitectura en Alta disponibilidad, permitiendo el despliegue tanto en modo Activo-Pasivo como Activo-Activo, sin necesidad de licencia
- Alta disponibilidad con sincronización de configuraciones y sesiones
- Interfaces reservados para gestión
- Posibilidad de configurar interfaces HeartBeat redundantes
- Identificación geográfica y posibilidad de aplicar políticas en función de esta, tanto de entrada como salida del tráfico internet
- Clasificación de todas las defensas frente a amenazas en base a riesgo y nivel de amenaza
- Posibilidad de definición de excepciones por defensa/firma, perfil, origen, destino y puerto.
- Capacidades de traffic shaping y priorización del tráfico, por aplicación, por política e interfaz y subinterfaz, tanto para el tráfico saliente como para el entrante siendo capaz de reservar ancho de banda y marcar el tráfico con DSCP
- Capacidad de proxy cache integrado en el mismo cortafuegos
- Opción de configuración de proxy explícito por interface, con posibilidad de hacer caching en caso de ser necesario
- Posibilidad de disponer de la funcionalidad de optimización WAN integrada en el propio cortafuegos
- Licencias ilimitadas
- Debe disponer de múltiples dominios de gestión (dominios administrativos) asociados a la estructura de dominios virtuales que se esté utilizando, ofreciendo tanto políticas específicas para cada dominio como políticas globales a todos los dominios
- Aplicación simultanea de políticas de seguridad en diferentes sistemas, dominios virtuales o clusters
- Sistema de revisión, chequeo y comprobación de la consistencia de las reglas de las políticas de seguridad, pudiendo verificarse la existencia de:
  - Duplicación de reglas y objetos
  - Reglas y objetos que son “ocultados” por otros
  - Reglas y objetos que son parcialmente sobrescritos por otros
  - Objetos definidos no utilizados

6.1.4 Especificaciones generales de seguridad

Los equipos ofertados deben cumplir con los siguientes requerimientos mínimos en cuanto a funcionalidades relativas a seguridad:

- Arquitectura basada en interfaces, para la aplicación de políticas de seguridad.

- Capacidad de identificación de aplicaciones a nivel 7 con un mínimo de 4000 identificadas (incluyendo aplicaciones Web 2.0), así como la identificación de subfunciones dentro de una aplicación como por ejemplo "compartir escritorio de webex", "chat dentro de webex", "transferencia de ficheros en webex", etc.
- Posibilidad de agrupación de las aplicaciones por categorías, de forma que las políticas de seguridad sean aplicadas por categorías de aplicaciones.
- Posibilidad de identificar las aplicaciones no solamente si utilizan los puertos tcp/udp por defecto o estándar sino en cualquier puerto que se utilice para dicha aplicación.
- Deben identificar aplicaciones propietarias que usen los protocolos HTTP, HTTPS y TCP.
- Capacidad para identificar las aplicaciones bajo túneles HTTPS
- Deben identificar aplicaciones que vayan bajo túneles encriptados SSL.
- Capacidad de definición de aplicaciones personalizadas.
- El Equipo de seguridad debe de permitir la creación de Aplicaciones personalizadas en función de atributos de capa7, para poder personalizar las posibles aplicaciones propietarias.
- Debe descifrar tráfico SSH y detectar aplicaciones no legítimas sobre este protocolo.
- Posibilidad de crear reglas de calidad de servicio según las aplicaciones que se usen en el tráfico.
- Posibilidad de aplicar políticas de NAT de forma independiente a las políticas de seguridad ante vulnerabilidades y de protección de la red interna.
- La solución debe incluir firmas, actualizaciones y tecnología propietaria. Como por ejemplo para las urls, malware, virus, firmas IPS, etc.
- Inspección de la identidad de la aplicación en cada establecimiento de conexión entrante o saliente
- Posibilidad de disponer de categorías master para facilitar la gestión de las políticas de filtrado.

6.1.4.1 Filtrado de URL

Los equipos ofertados deben filtrar la navegación http o https según la URL que se desea visitar basándose en diferentes criterios:

- Deben de definir manualmente listas estáticas de URL o de IP permitidas y no permitidas para la navegación, con posibilidad de definir para las no permitidas la acción a realizar (bloquear, permitir, pero advertir, generar solamente un log, etc.).
- Monitorizar y controlar la navegación web pudiendo trabajar con listas blancas y negras de URLs.
- Permitir la navegación basándose en categorías de URL, siendo dichas categorías actualizadas periódicamente a través de un servicio en la nube que permita al menos categorías de URL como "malware", "phising", "hacking", etc.
- Posibilidad de incluir listas de URL o IP dinámicas, de forma que los equipos puedan ser configurados para que de forma periódica consulten listas disponibles en servidores públicos reconocidos en los que se incluyen aquellas IP o URL relacionadas con amenazas y sean bloqueadas de forma automática.
- El equipo debe de proporcionar capacidades contra el robo de credenciales por ataques de Phising. De esta manera debe de ser capaz de:
- Bloquear sitios categorizados como phising.
- Alertar o Bloquear cuando una credencial de usuario interno vaya a ser publicada en un servicio externo a la red corporativa.
- Forzar doble factor de autenticación para las aplicaciones críticas, sean o no basadas en web.

Estas posibilidades deberán poder ser configurables mediante perfiles de forma que se puedan aplicar dichos perfiles a las reglas de tráfico tanto saliente como entrante de forma granular, permitiendo dicha aplicación a ciertos tipos de tráfico y no a otros.

- El equipo debe de ser capaz de mostrar una página de reemplazo personalizable para las páginas bloqueadas tanto en la navegación HTTP como HTTPS.
- El equipo debe de ser capaz de poder modificar los umbrales de configuración de alerta de un ataque de fuerza bruta.
- Base de datos de al menos 120 millones de URL.

6.1.4.2 Protección ante vulnerabilidades

Los cortafuegos ofertados deben contar con la posibilidad de aplicar políticas de protección ante vulnerabilidades y exploits tanto al tráfico entrante como al saliente, debiendo cumplir con las siguientes funcionalidades:

- Se debe poder aplicar políticas tanto de detección como de prevención (modo IDS o IPS) ante posibles exploits de vulnerabilidades que se detecten en el tráfico bien entrante o saliente de Internet sin incurrir en latencia superior a 1 milisegundo para no penalizar la sensación del usuario, efectuando el análisis en una única pasada para todo tipo de amenazas.
- En la protección ante vulnerabilidades el criterio a usar es la identificación de la aplicación que se usa para poder aplicar perfiles de vulnerabilidades ajustados a dicha aplicación, de forma que las prestaciones de los equipos no se vean mermadas.
- Los perfiles de detección y protección ante vulnerabilidades deben permitir ser aplicados tanto para el tráfico originado desde la red interna como para el tráfico originado desde Internet, debiendo ser posible la aplicación de detección y protección ante vulnerabilidades.
- Las vulnerabilidades deben estar categorizadas por tipos y por niveles de riesgo, de forma que la aplicación de perfiles de protección en el tráfico se pueda realizar en base a estas categorías.
- Se debe poder permitir usar la identificación CVE de vulnerabilidades para poder usar dicha identificación en la aplicación de perfiles de protección específicos.
- Utilización de la identificación de aplicaciones como criterio para seleccionar los perfiles de protección de vulnerabilidades, de forma que se apliquen solo aquellas firmas específicas según la aplicación que se está utilizando.
- Más de 11000 firmas disponibles para la funcionalidad de IPS.
- Funcionamiento como IPS basado tanto en patrones como en “Rated based”. Posibilidad de crear firmas de IPS customizadas
- Definición de las políticas de IPS por perfiles.
- Deberá permitir la creación de firmas específicas de IPS.

6.1.4.3 Antivirus

Los cortafuegos propuestos deben de definir políticas de antivirus, de forma que las descargas de ficheros realizadas en sentido Internet red Interna o viceversa sean inspeccionadas y bloqueadas si su contenido es malicioso.

El sistema antivirus debe de ser propietario del fabricante, de tal modo que no dependa de un tercero para la actualización de firmas.

Se debe poder aplicar políticas que permitan aplicar el motor de antivirus sobre protocolos como ftp, http, imap, pop3, smb o smtp, definiendo para cada uno de estos protocolos la acción a realizar (permitir los ficheros, descartar los ficheros, desconectar la sesión o registrar mediante logs) ante la detección del fichero

malicioso por el motor de antivirus, adicionalmente, se debe poder tener la posibilidad de enviar el fichero que se inspecciona a un servicio en Internet que permita el análisis de dicho contenido y emita un veredicto en caso de que el fichero sea malicioso que permita realizar al cortafuego las acciones oportunas.

Los cortafuegos deben permitir la aplicación de políticas de antivirus de forma granular, permitiendo por ejemplo la aplicación de dichas políticas a ciertos usuarios de determinados grupos o a ciertos segmentos de red con determinado direccionamiento o a ciertas aplicaciones.

6.1.4.4 Bloqueo de ficheros y datos sensibles

Los cortafuegos propuestos deben de identificar ficheros no basándose en su extensión sino en el tipo de contenido del archivo, permitiendo al menos 100 tipos de ficheros identificables.

Se debe poder aplicar políticas de bloqueo de ficheros basándose en su tipo, de forma que se pueda bloquear descargas de ciertos tipos de fichero o se permita su descarga pidiendo confirmación al usuario y se generen los logs correspondientes.

Los equipos propuestos deben poder ser capaces de aplicar políticas de bloqueo de ficheros atendiendo a criterios como origen y destino del tráfico, usuarios o grupos que originan las descargas, tipo de aplicación o de tráfico que genera las descargas de fichero y para el caso de navegación en internet se debe poder bloquear las descargas de ficheros cuando dicha navegación sea hacia URL categorizadas como peligrosas o que puedan suponer amenazas de seguridad.

Los equipos deben poder buscar patrones sensibles como combinaciones de números de tarjetas de crédito de forma que se evite la filtración de este tipo de datos.

- Detección del tipo de fichero por cabecera independientemente del tipo de extensión
- Capacidad de búsqueda de patrones como DNI, tarjetas de crédito, etc., así como a asociaciones concretas
- Soporte de lenguaje de descripción de datos para la personalización de DLP
- Posibilidad de definición de los tipos de dato en función de palabras clave, palabras clave ponderadas, expresiones regulares, atributos de fichero, diccionario, plantillas corporativas
- Detección e identificación de documentos mediante “Fingerprint”
- Posibilidad de añadir marcas de agua en los documentos de office
- Soporte de más de 75 categorías de filtrado de contenidos

6.1.4.5 Descifrado de tráfico SSL

Los equipos ofertados deben realizar como mínimo de las siguientes funcionalidades:

- Configuración de las autoridades certificadoras (CA) de confianza para la inspección de tráfico https.
- Identificar aplicaciones propietarias que usen los protocolos HTTP, HTTPS y TCP.
- Identificar aplicaciones que vayan bajo túneles encriptados SSL.
- Los cortafuegos ofertados deben descifrar tráfico SSL y SSH de forma granular, de manera que se puedan establecer políticas de descifrado basándonos en las zonas por las que viaja el tráfico, según las direcciones IP origen o destino del tráfico enviado, los usuarios que generan dicho tráfico o los puertos que se están usando para el envío de tráfico, pudiendo excluir categorías de sitios de internet a las que se accede del tráfico a descifrar.

6.1.4.6 Protección ante ataques de denegación de servicio

Los cortafuegos ofertados deben contar con medidas de protección ante ataques de Denegación de Servicio de forma que dichas medidas puedan ser activadas atendiendo a criterios como la zona o conjunto de interfaces desde donde se origina el tráfico, zona o conjunto de interfaces hacia dónde va dirigido el tráfico.

Se deberá contar al menos con los siguientes tipos de protección: SYN Flood, UDP Flood, ICMP Flood, ICMP Flood, protección ante inundaciones por nuevas sesiones, o protección por ataques de desborde por límites de sesiones establecidas, pudiendo en cada caso establecer los umbrales necesarios para activar dichas protecciones.

6.1.4.7 Detección de equipos comprometidos en la red

Los cortafuegos ofrecidos deben de detectar mediante firmas posibles equipos comprometidos en la red que intenten establecer comunicación con servidores de comando y control, permitiendo realizar acciones predeterminadas como bloquear o monitorizar y registrar mediante log este tipo de tráfico.

Entre las acciones posibles, se debe tener la capacidad de interceptar las peticiones de resolución de dominios realizadas desde servidores propios DNS internos a la red o hacia servidores DNS externos de forma que se identifique los equipos internos comprometidos por algún tipo de malware.

6.1.4.8 Tecnología de Sandboxing

Los cortafuegos propuestos deben tener la capacidad de disponer de un servicio en la nube o en on-premise capaz de analizar ficheros de tipo desconocido o enlaces URL recibidos en correos electrónicos, de forma que se permita el envío de dicha información para análisis atendiendo a criterios como:

- Tipo de aplicación que se está usando para transferir el fichero.
- Tipo de fichero que se está transfiriendo.
- Dirección de transferencia (descarga o subida de ficheros).

El servicio en la nube será capaz de analizar los siguientes tipos de ficheros: paquetes de aplicaciones Android, ficheros flash, applets java, ficheros de Microsoft office, ficheros ejecutables con formato PE incluyendo dll, ficheros pdf y enlaces HTTP y HTTPS incluidos en correos electrónicos recibidos por SMTP y POP3. El análisis realizado por este servicio en la nube en caso de que la información enviada sea categorizada como de tipo malicioso por suponer un riesgo de seguridad deberá generar las firmas apropiadas en un plazo de 5 minutos que se utilizarán para actualizar los motores propios de antivirus y filtrados URL de forma que las posteriores descargas de los mismos ficheros o URL enviadas sean bloqueadas por dichos cortafuegos.

Los cortafuegos deberán soportar el envío de logs y archivos al sandboxing por su interfaz de loopback.

Los cortafuegos deben tener la capacidad de enviar también al servicio de sandboxing en la nube no solamente aquellos ficheros de tipo sospechoso sino aquellos que hayan sido bloqueados por su propio sistema de firmas, con objeto de poder analizar variantes de malware e incorporar esas variantes al sistema de firmas de los propios motores del equipo, además se deberá poder consultar la información enviada y evaluada en la nube a efectos de generar los informes correspondientes.

6.1.5 Integración e identificación de usuarios

Cada firewall ofertado deberá tener las siguientes características técnicas relativas a gestión e identificación de usuarios, entendiéndose como funcionalidades mínimas a cumplir:

- Aplicación de políticas basadas en usuarios y grupos en vez de por ip.
- Integración con sistemas de directorios para obtención de usuarios y grupos, incluyéndose Microsoft Active Directory, Novell y eDirectory.

- Integración con sistemas multiusuario como Citrix o Microsoft Terminal Server para identificación de usuarios. Es decir, que el equipo sea capaz de identificar los múltiples usuarios conectados a un sistema de Microsoft Terminal Server o similar.
- Soporte de mensajes Radius Accounting para SSO.
- Autenticación en servidores remotos mediante LDAP, RADIUS y TACACS+.
- Capacidad de analizar mensajes de syslog con información de login y logout para identificación de usuarios.
- Posibilidad de inyectar usuarios mediante aplicaciones de terceros a través de API XML.
- Capacidad de poder identificar usuarios mediante portal de autenticación propio haciendo uso de protocolos como Kerberos, NTLM, SAML SSO, TACACS+, RADIUS, Certificados de Cliente o autenticación local.

6.1.6 Informes

Asimismo, los equipos cortafuegos proporcionados deben también tener la capacidad de generar informes tanto predefinidos como personalizados utilizando los logs generados por los propios equipos sin necesidad de equipos externos adicionales, limitándose dicha funcionalidad exclusivamente por la cantidad de logs que dichos equipos cortafuegos sean capaces de almacenar en su propio almacenamiento permanente.

Se debe disponer de la capacidad de generar informes de actividad por usuario, incluyendo aplicaciones utilizadas, sitios web visitados.

Se debe poder generar los informes de forma automática, así como agrupar varios informes en un único documento con formato PDF y que estos puedan ser enviado por correo electrónico a un grupo de distribución.

Entre los informes disponibles, se debe disponer de informes sobre los anchos de banda consumidos por las diferentes aplicaciones, informes sobre los orígenes y destinos geográficos de las amenazas detectadas, e informes sobre el análisis de comportamiento de tráfico observado que permita detectar equipos comprometidos participantes de botnets.

Los cortafuegos proporcionados deben permitir programar el momento en el cual se desea la generación del informe correspondiente y su envío a través de correo electrónico, así como el intervalo de fechas entre las cuales se desea la información de dicho report, dentro de las limitaciones de almacenamiento de los propios equipos.

Deberá ser fácil la generación de informes, y poder configurarlos en detalle. Se deberán identificar los enlaces (interlocutores, consumo, protocolos, etc) en tiempo real.

6.1.7 Procesamiento de logs

Los cortafuegos ofertados deberán tener la capacidad de almacenar los logs localmente con la única restricción de la capacidad de almacenamiento local del propio dispositivo o bien enviar los logs a una plataforma de gestión y procesamiento externa especializada con objeto de mantener dichos logs a largo plazo, el sistema de procesamiento de logs deberá cumplir con las siguientes características:

- Disponer de un cuadro de mando personalizable por usuario que accede al sistema con al menos la siguiente información: Aplicaciones más usadas, Aplicaciones de alto riesgo, Información general del sistema, Estado de los Interfaces, Logs relativos a las amenazas más observadas, Logs de filtrados URL o Recursos del sistema.
- Cuadro de mando de aplicaciones generado a partir de los logs, personalizable por usuario que permita disponer de información como los usuarios que más generan tráfico, las reglas de

seguridad que más se usan, vulnerabilidades que más se han detectado y bloqueado, equipos que navegan hacia dominios maliciosos, virus detectados, información enviada a los servicios de sandboxing o host comprometidos en la red interna.

- Deben usar el motor integrado de correlación de eventos dentro de la propia plataforma de forma que a partir de los logs recibidos se pueda obtener información de alto nivel como un listado de equipos comprometidos en la red interna y las evidencias que han dado lugar a dicho listado con indicación de tiempos, usuarios, direcciones ip y vulnerabilidades o amenazas detectadas.
- Posibilidad de filtrar cada una de las vistas o cuadros de mando de forma que la información esté restringida a ciertos criterios para poder realizar análisis más exhaustivos.
- Funcionalidad de consolidación de logs y diferentes niveles de agrupación (origen, destino, aplicación, amenaza, websites, etc.), para su visualización.
- Esta visualización tiene que ser tipo "Drill-down", es decir, poder seleccionar unos de los objetos agrupados e ir filtrando el resultado en base a esta selección, hasta saber el detalle completo.

6.1.8 Otras funcionalidades

Los cortafuegos propuestos deberán disponer de funcionalidades adicionales entre las que se encuentran:

- Posibilidad de definir aplicaciones y/o vulnerabilidades propias mediante diferentes parámetros como los puertos tcp o udp que se usan en dicha aplicación y combinaciones de patrones dentro de las cabeceras de los paquetes o en los propios payloads de dichos paquetes que se deben cumplir para que se reconozca la aplicación y/o vulnerabilidad.
- Los cortafuegos ofertados deben descifrar tráfico SSL y SSH de forma granular, de manera que se establezcan políticas de descifrado basándonos en las zonas por las que viaja el tráfico, según las direcciones ip origen o destino del tráfico enviado, los usuarios que generan dicho tráfico o los puertos que se están usando para el envío de tráfico, siendo posible excluir categorías de sitios de internet a las que se accede del tráfico a descifrar.
- Deben descifrar tráfico que pasa a través del cortafuegos destinado a sitios web que utilicen certificados de curva elíptica (ECC).
- Captura de tráfico. Los cortafuegos propuestos deben tener la capacidad de realizar capturas del tráfico que atraviesa sus interfaces en formato pcap, de forma que se puedan establecer criterios de la captura como capturar el tráfico originado por un cierto origen ip o destino, cierto puerto o también capturar tráfico de una aplicación en concreto independientemente del origen o destino del tráfico o incluso aplicar filtros de captura de tráfico exclusivamente cuando se detecte un virus o un ataque en los motores de protección.
- Los equipos cortafuegos deben de poder aislar los equipos que se encuentren en una DMZ, haciendo que el tráfico pase por el firewall y a través de sus reglas se permita cierto tráfico entre ellos. Por defecto los equipos, aunque estén en una misma VLAN no se verán entre sí.
- Los equipos deben de poder realizar microsegmentación, equipos que se encuentren en la misma red, con mismo rango de direccionamiento IP pertenezcan a distinta VLAN y el ARP se lleve hasta el firewall, sin necesidad de cambio de direccionamiento de los equipos ni configuración de private vlans, de modo que se pueda gestionar y limitar el tráfico entre ellos.
- Se requiere que el fabricante propuesto, figure en el apartado de líderes del cuadrante mágico de gartner, durante los últimos 5 años y/o que cuente con guías de configuración del CCN-CERT en cuanto a:
  - Configuración general de cortafuegos
  - Configuración de protección ante ataques DDoS

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.

Dicha tabla ha de presentarse como uno de los apartados en la oferta del licitador, rellenando la columna de referencia correspondiente a cada línea, pero sin incluir el importe económico de cada uno.

ID	REFERENCIA	DESCRIPCIÓN	CANT.
NUEVOS APPLIANCE SECURIZACIÓN-FIREWALL (ETAP IPARRAGUIRRE, OFICINAS BARAKALDO, OFICINAS GERNIKA, OFICINAS XUPERA, PRESA ORDUNTE, PRESA UNDURRAGA, ETAP BASATXU, ETAP GARAIZAR, ETAP GARTXETA, ETAP GOROZIKA, ETAP JARRALTA, ETAP OLETA, ETAP SALINILLAS, ETAP SAN CRISTOBAL, ETAP SAN MIGUEL, ETAP SAN SALVADOR, ETAP SOLLANO, OFICINAS BERMEO, OFICINAS BILBAO)			
1		Appliance securización (Firewall)	36

ID	REFERENCIA	DESCRIPCIÓN	CANT.
2		Licencias durante la duración del contrato de los equipos suministrados con funcionalidades de IPS, Protección Avanzada contra Malware (Antivirus, Botnets, Malware móvil, Sandbox…), Filtrado web y contenido, Filtrado DNS, DoS, Control de Aplicaciones	36
3		Soporte 24x7 fabricante RMA NBD anual durante toda la duración del contrato	36

ID	REFERENCIA	DESCRIPCIÓN	CANT.
4		Soporte integrador 24x7x4 anual durante la duración del contrato de los equipos suministrados	36
SERVICIOS GENERALES			
5		Replanteo de instalaciones	1
6		Asistencia técnica migración equipos de seguridad perimetral	1
7		Documentación	1
8		Documentación esquemas eléctricos	
9		Servicio de monitorización externa (NOC)	1
10		Bolsa de Horas de 50 horas por año de contrato	1
OTROS MATERIALES			

ID	REFERENCIA	DESCRIPCIÓN	CANT.
11		Pequeño material: bandejas, schuko, tomacorrientes, panel fibra, patch panel UTP, carril DIN, pletinas para tierras, tapas ciegas, pasahilos, etc	1
12		Latiguillos Cable Ethernet CAT6A	20
13		Latiguillos de fibra óptica MULTIMODO	20

Nota: Respecto a los ítems 12 y 13, los latiguillos podrán ser de 2,3 5 o 10 metros, según necesidades.