



Ayuntamiento
de Vitoria-Gasteiz
Vitoria-Gasteizko
Udala

www.vitoria-gasteiz.org

Número de Expediente: 2024/CO_ASUM/0009

ASUNTO: PLIEGO TECNICO DEL EXPEDIENTE DE CONTRATACIÓN DEL SUMINISTRO DE EQUIPAMIENTO DE SEGURIDAD

1. INTRODUCCIÓN

El Departamento de Modernización de Administración del Ayuntamiento de Vitoria-Gasteiz, cuenta como parte de la infraestructura de seguridad con un cluster de Firewall Fortigate 600D que llega a su fin del ciclo de vida de fabricante en 2024. Mediante el presente pliego se va a solicitar oferta para la adquisición y configuración del equipamiento del mismo fabricante que permita sustituirlo de manera ágil, además de dotar de una nueva capa de seguridad a las comunicaciones con el Ayuntamiento.

2. OBJETO DEL CONTRATO

El objeto del contrato es el suministro, configuración y puesta en marcha de una pareja de Firewalls en cluster que reemplace el cluster actual con su mantenimiento y soporte durante tres años.

Adicionalmente, también es objeto del contrato el suministro de licencias y servicios adicionales relacionados con el Zero Trust Network Access (Acceso a la red de confianza cero) para ampliar y mejorar los recursos de seguridad del Ayuntamiento en las conexiones remotas a las redes y servicios internos.

Para ello, es preciso ejecutar las siguientes actuaciones en los términos del presente pliego:

- Suministro de una pareja de Firewalls.
- Suministro de la óptica necesaria para la instalación del cluster de Firewall
- Suministro de las licencias Forticlient ZTNA y servidor Forticlient EMS necesarios para la puesta en marcha de una arquitectura ZTNA.
- Proyecto de migración del cluster de Firewalls para reemplazar el cluster actual.
- Puesta en marcha del nuevo cluster de Firewalls.
- Proyecto de instalación de la arquitectura ZTNA
- Puesta en marcha de la arquitectura ZTNA



- Formación, tanto sobre el cluster de Firewall, como de la arquitectura ZTNA desplegada.
- Garantía y mantenimiento de todo el equipamiento y licencias suministradas.

3. SITUACIÓN ACTUAL

En la actualidad el Ayuntamiento dispone de la pareja de Firewalls FortiGate 600D configurados en cluster. Cada uno de los miembros del cluster se encuentra físicamente en diferentes dependencias municipales con conexión de fibra propia municipal entre sí, lo que nos permite tener extendida la red entre ambas dependencias. Cualquier subred conectada al firewall activo, puede llegar también al firewall pasivo y por tanto una puerta de enlace puede estar configurada en alta disponibilidad en el cluster de firewalls.

La configuración del cluster será activo-pasivo.

Ambos firewalls tienen actualmente dos enlaces de **una** sola fibra 10Gb a dos equipos de switching diferentes. Cada firewall tiene por tanto:

- 1 enlace de fibra 10Gb con un switch “A”.
- 1 enlace de fibra 10Gb con un segundo switch distinto al anterior “B”.

Entre las funcionalidades y servicios que se están utilizando a día de hoy en el Firewall 600D están las siguientes:

- FortiCare Support
- Políticas de firewall generalmente basadas en interfaz, origen, destino, servicio
- NATs de salida para ciertas políticas de las anteriores.
- Rutas estáticas
- Security profiles para las reglas de firewall de:
 - Antivirus
 - Web Filter con múltiples Web Rating Overrides
 - DNS Filter
 - AppControl
 - Intrusion Prevention
 - SSL/SSH Inspection con rotura de túnel para el filtrado Web.
- Fabric Root del Security Fabric del Ayuntamiento.



- Conexión con FortiAnalyzer
- Conexión con FortiSandbox Cloud
- Conexión con Windows AD mediante FSSO Agent
- Threat Feeds (IOCs, listas de IPs, listas de dominios, etc.)
- Web proxy transparente con rotura de tunel SSL.
- Configuración en HA
- Definición de varios UserGroup vinculados a grupos de Windows AD mediante FSSO.
- Autenticación en el propio Firewall mediante usuarios de dominio específicos, bien administradores de control total o usuarios de solo lectura.

4. SITUACIÓN OBJETIVO

Por un lado, respecto a los Firewalls, la situación objetivo es disponer de un nuevo cluster Fortigate 600F que reemplacen los actuales Fortigate 600D. Por ello, la situación objetivo a nivel lógico es, en base, la misma que la actual, pero con el nuevo equipamiento.

A nivel físico, sin embargo, si que se pretende mejorar las conexiones para dotar de una mejor estabilidad en caso de caídas de enlace. Por ello, el objetivo es tener como mínimo un doble enlace agregado (LACP) de 10Gb en cada firewall de la pareja. Cada par de enlaces va hacia stacks o pila de switches diferentes.

Cada miembro de la pareja del firewall, por tanto, tendrá los siguientes enlaces:

- 2 enlaces de fibra 10Gb agregados en LACP con un primer switch lógico (stack) "A" por fibra multimodo.
- 2 enlaces de fibra 10Gb agregados en LACP con un segundo switch lógico (stack) "B", una fibra por monomodo y otra por multimodo.

Las distancias de las conexiones multimodo son menores a 300 metros (10GBase-SR) y las conexiones monomodo son menores de 10 kilómetros (10GBase-LR).

Por otro lado, se requiere poner en marcha una arquitectura ZTNA para securizar las conexiones entrantes. Como actualmente se está utilizando tecnología Fortinet como cliente VPN para el acceso remoto, el objetivo es implementar un servidor EMS on-premise, donde poder establecer los perfiles necesarios que garanticen que los clientes que se conectan mediante Forticlient EMS son seguros.

5. TAREAS A REALIZAR POR LAS EMPRESAS LICITANTES

En este apartado se describen las tareas que deben realizar las empresas licitantes



5.1. SUMINISTRO DE FIREWALLS

Las empresas licitadoras deberán suministrar una pareja de firewalls Fortigate 600F para montar un cluster que puedan reemplazar a los Firewalls 600D cumpliendo la solución objetivo.

La empresa suministrará también un latiguillo UTP para cada conexión de sincronismo y para consola que haya que realizar por cobre, siendo responsabilidad del Ayuntamiento el suministro del latiguillos adicionales en caso de que haya que utilizar parcheos a paneles intermedios.

5.2. SUMINISTRO DE LICENCIAS DE FIREWALL Y FORTICLIENT ZTNA

Se debe suministrar como parte del presente contrato las licencias de Fortigate con soporte FortiCare Premium y con los mismos servicios de los que se dispone en la actualidad en el Firewall 600D durante tres años desde el inicio del contrato, como son:

- FortiCare Premium
- IPS
- AV
- Web Filter
- Email Filtering
- Outbreak Prevention
- FortiSandbox Cloud.

Además se requiere la licencia para los mismos tres años de las siguientes licencias de seguridad Fortinet adicionales:

- FortiClient VPN/ZTNA Agent. Suscripción para al menos 100 endpoints
- FortiClient EMS on-premise con FortiCare Premium.

El FortiClient EMS deberá ser suministrado virtualizado para instalar en la virtualización municipal (VMWare). Los recursos hardware de virtualización correrán a cargo del Ayuntamiento de Vitoria-Gasteiz.

Todas las licencias deberán ser propiedad del Ayuntamiento de Vitoria-Gasteiz y suministradas a la cuenta del Ayuntamiento de Vitoria-Gasteiz. En caso de ser necesario, el Ayuntamiento proporcionará la cuenta a la que agregar las licencias a la empresa adjudicataria.

5.3. SUMINISTRO DE OPTICA



El suministro de la óptica debe realizarse teniendo en cuenta que no se pueden reutilizar las ópticas actuales para montar los nuevos enlaces en paralelo y poder realizar la migración con garantías y con el mínimo corte.

Por tanto, las empresas licitadoras deberán suministrar toda la óptica de los Firewalls, incluyendo algunas ópticas correspondientes a los switches de las que no dispone el Ayuntamiento.

Las ópticas a suministrar por parte de la empresa adjudicataria del lado de los Firewall son las siguientes:

- 6 ópticas Fortinet 10G SFP+ LC SR MMF (multimodo) para los Fortigate 600F
- 2 ópticas Fortinet 10G SFP+ monomodo hasta 10Km. para los Fortigate 600F

Las ópticas a suministrar por parte de la empresa adjudicataria para el lado de los switches municipales son las siguientes

- 2 ópticas Aruba 10G SFP+ LC LR hasta 10Km SMF (monomodo) para switches Aruba 6300M (part number del SFP+: J9151E)
- 2 ópticas Aruba 10G SFP+ LC SR MMF (multimodo) para switches Aruba 6300M (part number del SFP+: J9150D)

El Ayuntamiento ya dispone las otras 4 ópticas 10G LC SR multimodo restantes para los 4 enlaces faltantes.

La empresa adjudicataria deberá suministrar también todos los latiguillos de conexión de fibra multimodo firewall-switch dentro del propio CPD (latiguillos LC-LC duplex OM3 3m), así como los latiguillos de fibra monomodo para conectar los firewall y los switches Aruba con los paneles fibra de salida de cada edificio (latiguillos SC/UPC-LC duplex OS2 3m). Todos los paneles de salida monomodo son conectores SC-UPC.

Será necesario suministrar los latiguillos para todos los enlaces, incluyendo aquellos para los que la óptica sea proporcionada por el Ayuntamiento. Sin embargo, será responsabilidad del Ayuntamiento garantizar la continuidad de las fibras desde los CPDs hasta los switches Aruba ubicados fuera de los CPDs.

Todas las ópticas deben cumplir los siguientes requisitos:

- Nuevo y original de fabricante (Fortinet y Aruba, según el caso).
- Comprado en Europa mediante canal de fabricante
- Deben ser soportadas oficialmente por los respectivos fabricantes (Fortinet y Aruba) para ser utilizados en su respectivo equipamiento. Será motivo de no aceptación aquellas ofertas que ofrezcan ópticas no autorizadas por fabricante o que puedan invalidar la garantía y el soporte de mantenimiento de las tecnologías de switching.



Se deben suministrar todas las ópticas de los nuevos enlaces, no siendo válido reutilizar las ópticas de los Fortigate 600D actuales para facilitar la migración.

5.4. PUESTA EN MARCHA DE LOS FIREWALLS

Las empresas licitadoras deben incluir en sus propuestas un proyecto de migración de Firewall en el que se especificará las distintas tareas y fases a realizar para la consecución de la migración desde la situación inicial de los Firewall a una situación en la que el nuevo cluster de Firewall esté completamente operativo.

La empresa adjudicataria realizará la migración descrita en el proyecto con la supervisión municipal, acordando en todo momento con los técnicos municipales las ventanas de cambio necesarias para minimizar el impacto en los servicios.

Para la instalación física contarán con la ayuda de técnicos municipales para buscar el lugar apropiado y para realizar las conexiones dentro del CPD. La conexión a los switches se hará bajo la supervisión de técnicos municipales en coordinación con la empresa adjudicataria.

La empresa adjudicataria deberá, igualmente, realizar las pruebas especificadas en el proyecto de migración para garantizar que la puesta en marcha ha sido satisfactoria.

5.5. PUESTA EN MARCHA DE LA ARQUITECTURA ZTNA

La empresa adjudicataria deberá activar el licenciamiento necesario para implantar la nueva arquitectura ZTNA. El licenciamiento será agregado a la cuenta Fortinet que tiene el Ayuntamiento de Vitoria-Gasteiz.

Se deberá poner en marcha el servidor EMS on-premise virtualizado y realizar una configuración base de perfiles en FortiClient ZTNA en los términos en los que se determine por los técnicos municipales.

Además se realizarán pruebas para validar que la solución está operativa.

5.6. FORMACIÓN

La empresa adjudicataria deberá realizar una sesión de formación y demostración del equipamiento suministrado incluyendo, como mínimo, lo siguiente:

- Configuración realizada en los nuevos Firewall.
- Nuevas funcionalidades de la nueva versión de Firewall.
- Configuración del FortiClient EMS
- Configuración de los agentes FortiClient.
- Tareas de operación más habituales.



La formación se realizará, preferentemente, de forma presencial en las instalaciones del Ayuntamiento y en ningún caso tendrá una duración inferior a 4 horas.

5.7. GARANTÍA Y MANTENIMIENTO DEL MATERIAL SUMINISTRADO

Las empresas licitadoras deberán ofrecer una **garantía de fabricante de tres años desde la formalización del contrato**, para todo el suministro hardware y software.

Una vez puesto en marcha el nuevo equipamiento, se debe ofrecer además un **servicio de mantenimiento** de los Firewalls Fortigate, el servidor FortiClient EMS y los agentes Forticlient ZTNA que tenga la misma duración que el periodo de garantía.

Servicios requeridos:

- Resolución de incidencias: en caso de incidencia, la empresa adjudicataria realizará las acciones necesarias para recuperar en el menor tiempo posible la operativa normal del servicio.

Asimismo, la empresa adjudicataria realizará todas las tareas de intermediación con el fabricante necesarias para la resolución de las incidencias.

- Actualizaciones de fabricante:
 - La empresa adjudicataria realizará las actualizaciones a la última versión estable del sistema operativo o firmware recomendada por el fabricante. La carga de estos elementos se deberá realizar en un plazo no superior a tres meses después de su publicación oficial.
 - La empresa adjudicataria instalará todas las actualizaciones de seguridad publicadas por fabricante para corregir vulnerabilidades a la mayor brevedad posible y siempre, salvo cuando se llegue a un acuerdo distinto con los técnicos municipales, en un tiempo inferior a 5 días desde su publicación.
- Retirada y reciclado: la empresa adjudicataria deberá retirar y reciclar todos los equipos y componentes sustituidos como parte de los trabajos realizados para la resolución de incidencias.

Formato de los servicios:

- Los servicios asociados al mantenimiento se llevarán a cabo, de forma habitual, en remoto a través de VPN desde las instalaciones del adjudicatario.
- Cuando no sea posible el soporte remoto, los técnicos de la empresa adjudicataria se trasladarán a las instalaciones del Ayuntamiento de Vitoria-Gasteiz.
- De manera específica, se realizarán de forma presencial ciertas tareas de gestión del servicio que se acordarán entre el Ayuntamiento de Vitoria-Gasteiz y la empresa adjudicataria.



- Los costes asociados al desplazamiento de los técnicos correrán por cuenta de la empresa adjudicataria.

Gestión del servicio:

- Las empresas licitadoras incluirán en sus propuestas un servicio de ventanilla única para las comunicaciones entre proveedor y Ayuntamiento de Vitoria-Gasteiz.
- Las empresas licitadoras deberán indicar en sus propuestas las herramientas de gestión y los recursos de los que dispone para poder atender incidencias y realizar informes.
- Cualquier acción realizada en el marco del servicio deberá quedar debidamente documentada y registrada en la herramienta de gestión asociada al servicio de ventanilla única.
- Las empresas licitadoras deberán aportar en sus propuestas el procedimiento detallado para la gestión de incidencias, desde la comunicación de las mismas por parte del Ayuntamiento de Vitoria-Gasteiz, a la consulta para su seguimiento y hasta su cierre.
- Las empresas licitadoras deberán aportar en sus propuestas el procedimiento detallado para la gestión de las actualizaciones de fabricante.
- Las empresas licitadoras deberán aportar en sus propuestas el procedimiento detallado para la gestión de la retirada y reciclado de equipos y componentes sustituidos como parte de los trabajos realizados para la resolución de incidencias.

Personal asignado:

- La propuesta deberá incluir el detalle del equipo de trabajo
- El equipo de trabajo a incorporar tras la formalización del contrato para la ejecución de los trabajos deberá ser el detallado en la oferta adjudicataria y consecuentemente valorado.
- La empresa adjudicataria no podrá subcontratar con terceros la prestación de los servicios que se contratan sin la previa comunicación y consentimiento expreso por escrito del Ayuntamiento de Vitoria-Gasteiz. Aunque se produzca la subcontratación consentida, el adjudicatario responderá frente al Ayuntamiento de Vitoria-Gasteiz de la total ejecución del contrato, sin perjuicio de la responsabilidad del subcontratista.
- El adjudicatario procederá a la sustitución del técnico o técnicos asignados, a petición del Ayuntamiento de Vitoria-Gasteiz por motivos justificados.
- La sustitución de alguno de los técnicos asignados por parte del adjudicatario deberá ser realizado previa presentación del currículum del nuevo personal y con la aprobación del Ayuntamiento de Vitoria-Gasteiz.



- En los períodos vacacionales y/o bajas, el servicio se mantendrá en las mismas condiciones descritas, debiendo el adjudicatario disponer para ello de otros técnicos, debidamente asesorados, de características similares al que falte.
- El Ayuntamiento de Vitoria-Gasteiz proporcionará el acceso a los distintos edificios municipales a los técnicos asignados para dar el mantenimiento. Los técnicos de la empresa irán acompañados por personal técnico del Ayuntamiento de Vitoria-Gasteiz para poder acceder a los CPDs.

Horario del servicio:

Se definen 2 horarios para el servicio:

- Horario punta: lunes a viernes laborables de 8:00 a 15:00.
- Horario valle: resto.

Nivel de servicio:

- Se distinguen 3 niveles de criticidad para las incidencias:
 - Baja: degradación apreciable de algún servicio auxiliar no importante aún cuando siga operativo. No se ve afectado ningún servicio importante.
 - Media: pérdida de algún servicio auxiliar no importante o degradación apreciable de algún servicio importante aún cuando siga operativo.
 - Alta: pérdida completa de uno o más servicios importantes.
- Corresponde a los técnicos municipales establecer el nivel de criticidad de cada incidencia.
- El nivel de servicio se establece en función del nivel de criticidad de las incidencias y del horario de trabajo:

Criticidad	Horario punta		Horario valle	
	T. de respuesta	T. de resolución	T. de respuesta	T. de resolución
Alta	< 1 hora	< 6 horas	< 2 horas	< 8 horas
Media	< 2 horas	< 8 horas	< 3 horas	< 24 horas
Baja	< 3 horas	< 24 horas	-	-

T. de respuesta: tiempo transcurrido desde la comunicación de la incidencia hasta que los técnicos encargados de la resolución comienzan los trabajos de diagnóstico.

T. de resolución: tiempo trascurrido desde la comunicación de la incidencia hasta su resolución.

Nivel de cobertura

- La empresa adjudicataria ofrecerá un servicio en modo 24x7 acorde con el nivel de servicio de la tabla anterior.



6. ENTREGABLES A LA PRESENTACIÓN DE LAS OFERTAS

En este apartado se describen los entregables que presentarán las empresas licitadoras como parte de sus propuestas técnicas.

6.1. PROYECTO DE MIGRACIÓN DE FIREWALL

Las empresas licitantes deben entregar un plan de proyecto de la migración de Firewalls.

En el proyecto se propondrá un equipo de trabajo integrado por personal de la empresa licitadora y por personal del Ayuntamiento de Vitoria-Gasteiz cuyo objetivo será llevar a término el proyecto de manera eficaz y eficiente.

Para la elaboración del proyecto, se debe tener en cuenta todo lo necesario para llevar a cabo el trabajo de migración y en el que se incluyan todo lo siguiente:

- Detalle del equipo de trabajo para el proyecto de migración del Firewall.
- Se debe especificar de manera detallada los pasos a seguir para la migración de todos los servicios que están funcionando en los firewalls actuales.
- Se deben identificar las distintas ventanas de corte con su duración y su ámbito. Es deseo del Ayuntamiento minimizar el número de ventanas, minimizar su duración y poder acotar su ámbito para que la migración esté más controlada.
- Se deben identificar el mecanismo de copias de seguridad.
- Se deben establecer una fase de pruebas y detallar las distintas pruebas a realizar.

En el caso de pasos críticos se debe prever una vuelta atrás para en caso de fallo.

Dentro del proyecto se deben identificar los hitos y tareas, así como un cronograma en el que se ordenen en el tiempo las tareas del proyecto con sus dependencias.

También se deben tener en cuenta cuestiones relevantes como:

- Montaje en paralelo para facilitar la migración
- Fases o pasos para migrar todos los servicios: reglas, filtrados, servicios de seguridad, rutas, etc.
- Tiempos de corte de servicio, minimizando el número de cortes y minimizando el tiempo de duración de los mismos.
- Agregación de enlaces hacia ambos dominios de switches para maximizar el ancho de banda y para dotar de mayor escalabilidad a los mismos.



- Para cada tarea crítica se debe identificar una posible vuelta atrás en caso de incidencia o problemas.

Como parte final del proyecto, se debe aportar un plan de pruebas en las que se pueda comprobar el correcto funcionamiento de la funcionalidad básica del firewall y de los mecanismos de alta disponibilidad.

Además, se debe incluir la documentación técnica de fabricante de los dispositivos suministrados en la que quede claro que cumplen con los requisitos exigidos en los apartados anteriores.

6.2. PROYECTO DE INSTALACIÓN DE LA ARQUITECTURA ZTNA

Se debe proporcionar un proyecto de instalación de Forticlient EMS y puesta en marcha de los perfiles base de Forticlient ZTNA en los términos que se describen en el apartado correspondiente.

6.3. PLAN DE FORMACIÓN

Se debe entregar un plan de formación en los términos que se describen en el apartado correspondiente

6.4. DOCUMENTACIÓN DEL SERVICIO DE GARANTÍA Y MANTENIMIENTO

Esta documentación debe incluir todo lo solicitado en el apartado de garantía y mantenimiento del material suministrado.

Debe asegurarse que se incluyen las siguientes partes:

- Identificación del servicio de ventanilla para comunicación de incidencias.
- Detalle de las herramientas de gestión y los recursos de los que dispone para poder atender incidencias y realizar informes.
- Procedimiento detallado para la gestión de incidencias, desde la comunicación de las mismas por parte del Ayuntamiento de Vitoria-Gasteiz, a la consulta para su seguimiento y hasta su cierre.
- Procedimiento detallado para la gestión de las actualizaciones de fabricante.
- Procedimiento detallado para la gestión de la retirada y reciclado de equipos y componentes sustituidos como parte de los trabajos realizados para la resolución de incidencias.
- Detalle del equipo de trabajo para el servicio de mantenimiento.



7. REQUISITOS ADICIONALES

Aquellos trabajos (que no supongan cortes de servicio) que requieran la participación de los técnicos municipales para su ejecución o las tareas que ejecute la empresa adjudicataria en las instalaciones del Ayuntamiento de Vitoria-Gasteiz se realizarán en horario laboral municipal. Esto es, de lunes a viernes de 7:30 a 15:00.

Si fuera necesario, se podrían planificar trabajos fuera del horario laboral municipal siempre que se cuente con la aprobación de los técnicos municipales.

En caso de trabajos o tareas de la migración que supongan corte de servicio se acordará con los técnicos municipales la mejor franja horaria para minimizar la afección.

Los trabajos que la empresa adjudicataria ejecute en remoto y para los que no necesite la participación de técnicos municipales podrán ser realizados en el horario que decida la empresa adjudicataria, siempre que se cuente con la aprobación de los técnicos municipales.

Además, se deben cumplir los siguientes requisitos generales adicionales a todos los suministros del presente contrato:

- Todo el hardware ofertado se entregará con la última versión de sistema operativo o firmware disponible a la fecha de la adjudicación del concurso.
- Se especificará marca y modelo de todos los componentes hardware ofertados.
- Se requiere equipamiento nuevo y original de fabricante.
- No se admitirán equipos de segunda mano ni reacondicionados (refurbished) por el fabricante.
- No se admitirán propuestas con equipamiento cuyo End of Life haya sido anunciado por el fabricante.
- Corre por cuenta de la empresa adjudicataria la provisión de cualquier elemento necesario para la instalación y conexión de los nuevos firewalls (tornillería, cableado, fibras ópticas...).