24-8-16

PLIEGO DE CONDICIONES TÉCNICAS PARA EL SUMINISTRO, MANTENIMIENTO Y SOPORTE DE LA INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL DE LA RED MUNICIPAL DEL AYUNTAMIENTO DE SAN SEBASTIÁN DE LOS REYES

C.I.F.: P-2813400-E

TOMÁS SANZ ROMERO
TÉCNICO DE SISTEMAS
NUEVAS TECNOLOGÍAS

JORGE IZQUIERDO ALONSO
TÉCNICO DE SISTEMAS
NUEVAS TECNOLOGÍAS

FERNANDO PRATS SEVILLA
JEFE DE SISTEMAS DE INFORMACIÓN
NUEVAS TECNOLOGÍAS

Índice

C.I.F.: P-2813400-E

1 OBJETO

El presente pliego tiene por objeto definir las especificaciones técnicas que regirán en la contratación del suministro de la infraestructura y servicios necesarios para acometer la renovación tecnológica de la plataforma de seguridad perimetral de la red corporativa municipal, así como el soporte y mantenimiento de forma unificada de todos aquellos elementos implantados como resultado de la ejecución de este pliego.

En el presente documento quedarán definidas las necesidades técnicas a satisfacer por el oferente durante la ejecución del contrato para llevar a cabo esta renovación tecnológica, su mantenimiento y el soporte asociado a facilitar durante el periodo de ejecución que se extienda dicho contrato.

2 ALCANCE DEL SERVICIO

El contrato objeto del presente pliego incluirá los siguientes conceptos:

a) Renovación tecnológica del equipamiento de seguridad perimetral y elementos de interconexión a red pública con el que actualmente cuenta el Ayuntamiento de San Sebastián de los Reyes (en adelante Ayuntamiento) lo que incluirá:
    - Suministro, configuración y puesta en marcha del sistema de cortafuegos perimetrales para la protección de la red corporativa y DMZ frente a redes de conexión externa (públicas y red privada interadministrativa). Esta nueva solución sustituirá a la infraestructura actual existente en el Ayuntamiento (2xStoneGate) que se detalla más adelante, teniendo que cumplir con las exigencias y requisitos técnicos demandados.
    - Suministro, configuración y puesta en marcha de solución de entrega segura de correo electrónico para los servidores municipales (antivirus y antispam). Esta nueva solución sustituirá a la infraestructura actual existente en el Ayuntamiento (2xIronport), detallada más adelante, y deberá cumplir las exigencias y requisitos técnicos demandados.
    - Suministro e implantación de una nueva infraestructura de cortafuegos que suponga una segunda capa de protección en el acceso a la red de servidores corporativos (backoffice) separándola de las redes de usuarios del Ayuntamiento.

b) Mantenimiento y soporte de toda la infraestructura por un proveedor único experto en seguridad de sistemas de información, con capacidad de asesoramiento técnico en las distintas problemáticas, así como en la adecuación de la infraestructura al cumplimiento de los requerimientos demandados en el Esquema Nacional de Seguridad (ENS).

c) Centralización y simplificación en la gestión y control de las infraestructuras de seguridad perimetral incorporadas en el nuevo escenario así como mejora en las herramientas de gestión y consulta de eventos de cada una pudiendo incorporarse como herramientas de correlación de eventos para generación de alertas de seguridad.

3 REQUISITOS PARA LA RENOVACIÓN TECNOLÓGICA

Se plantea en el presente proyecto, la mejora y evolución tecnológica de los diversos sistemas de seguridad con los que cuenta actualmente el Ayuntamiento con los siguientes objetivos a conseguir:

- Redefinición de la arquitectura actual de conexión optimizando los recursos y corrigiendo problemas en el aislamiento de la DMZ detectados en auditoría, separando físicamente interfaces de conexión de cortafuegos y dotando de mecanismos de alta disponibilidad a la electrónica de red de interconexión.
- Unificación de la navegación corporativa centralizando su salida, control de acceso y filtrado de contenidos y mejorando el nivel de trazado de las conexiones. Mejora del rendimiento de navegación mediante *caching* (proxy) en los propios cortafuegos.
- Mejora en la seguridad perimetral para protección de servicios públicos (servicios web, correo, etc.) ***incorporando capacidades de nivel 7 en los servicios de cortafuegos,*** así como otros sistemas de detección temprana de amenazas (IDS, IPS, etc.).
- Revisión y mejora de la infraestructura de ***seguridad en entrega y recepción del correo electrónico con capacidades de antispam, antivirus y detección avanzada de amenazas***, actualmente soportada por equipamiento de hardware dedicado.
- Aumento en el control y seguridad interna mediante la ***incorporación de una nueva capa de cortafuegos, que permita separar y controlar el acceso a servidores internos,*** previniendo contra ataques, tanto desde el exterior como desde la propia organización de la red de usuarios. La infraestructura de servidores municipal está completamente virtualizada bajo Vmware, por lo que puede contemplarse para esta parte una solución de *appliance* virtual de seguridad.

3.1 Infraestructura actual

Los equipos con los que cuenta el Ayuntamiento para la prestación del servicio y funcionalidades de seguridad perimetral de su red corporativa municipal son los siguientes:

- Dos equipos cortafuegos Stonegate en configuración redundante activo/pasivo que separan las redes de acceso a Internet de la red municipal y protegen el perímetro para los servicios de correo electrónico, web corporativa municipal y servicios web ofrecidos al ciudadano. Además permiten la conexión VPN a la red corporativa a empleados y proveedores con las siguientes funcionalidades:
    - Filtrado y securización de red DMZ y red interna protegiendo servicios web, correo electrónico y accesos remotos externos mediante reglas de acceso y denegación IP y puerto (TCP/UDP)
    - Reglas de NAT por interfaz para ofrecer servicios externos y permitir conexiones entrantes de proveedores.
    - Reglas de QoS y control de estado de los enlaces para definir rutas alternativas (*multilkink*)
    - Gestión de túneles IPSec para conexión VPN con la red interadministrativa/SARA de la AGE y la red VPN de usuarios.
    - Consulta de capacidades del equipamiento en hojas de especificaciones del producto, según se recoge en el Anexo 1.

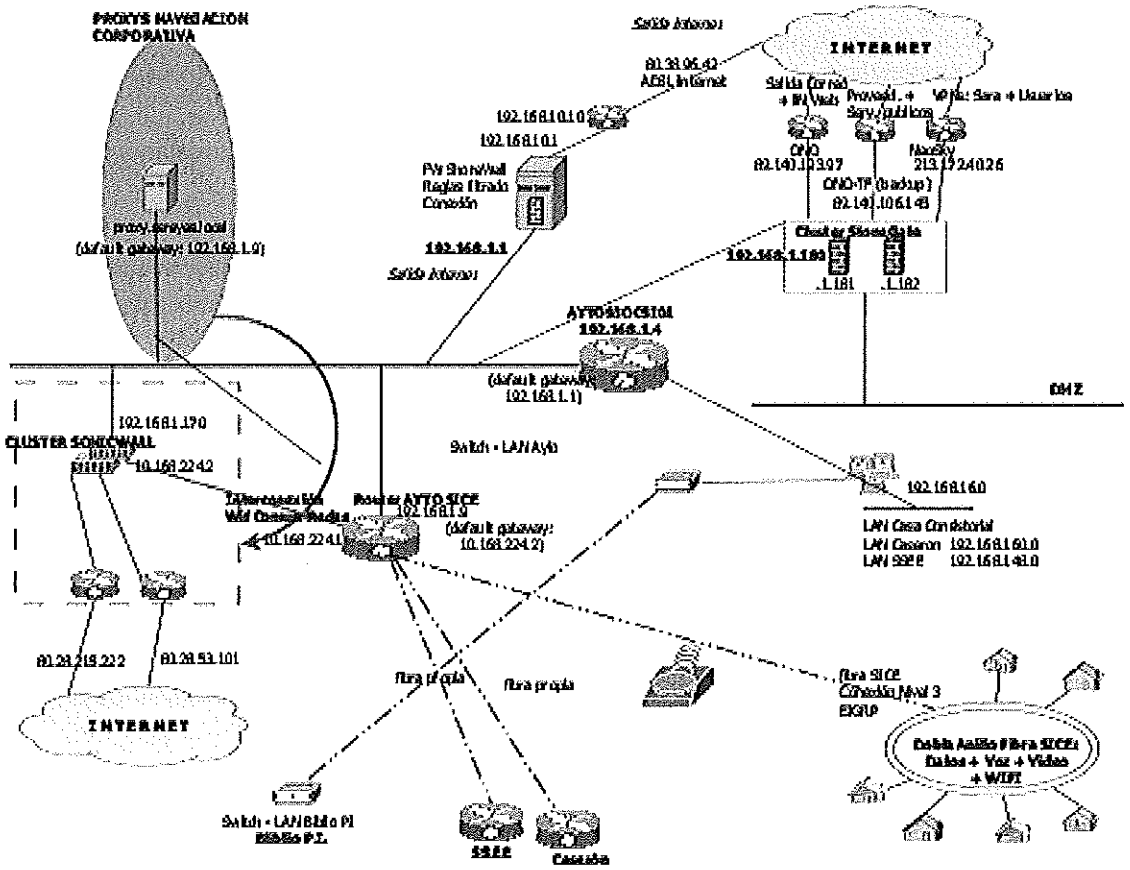
- Dos equipos cortafuegos Sonicwall en configuración redundante, que permiten la conexión de los empleados municipales a Internet, principalmente para navegación y conexión a distintos servicios en la nube, con las siguientes funcionalidades:
    - Filtrado y securización en el acceso a Internet de los empleados municipales a través de la definición de reglas de control de acceso TCP/IP y UDP
    - Filtrado y control de accesos en la navegación web corporativa, mediante el filtrado de direcciones URL basado en bases de datos de categorización de las mismas.
    - Filtrado y securización a nivel 7, mediante control de aplicaciones en el acceso a Internet y ataques externos.
    - Consulta de capacidades del equipamiento en hojas de especificaciones del producto, según se recoge en el Anexo 1.

- Dos equipos *antispam* y *antivirus* de correo Ironport en alta disponibilidad, realizando las funciones de *relay* y control de correo, tanto entrante como saliente, con las siguientes funcionalidades:
    - Filtrado de correos basado en reputación de IP, reglas heurísticas, listas blancas y listas negras.
    - Gestión de cuarentena a nivel de buzón de usuario. Integración de sistema de gestión de usuarios con directorio activo
    - Administración centralizada de ambos equipos en cluster desde interfaz web
    - Consulta de capacidades del equipamiento en hojas de especificaciones del producto, según se recoge en el Anexo 1.

- Una máquina virtual a modo de servidor proxy http, basado en software libre Squid 3, para la navegación corporativa de los empleados municipales, que permite *caching* de contenidos y control de navegación de los usuarios.

En el Anexo 1 del presente pliego se puede ver una descripción más detallada de estos elementos, así como sus condiciones de licenciamiento vigentes.

La siguiente figura muestra, de forma simplificada, el esquema de red en el que aparecen reflejados cada uno de los elementos que componen la infraestructura de seguridad perimetral actual descrita:



3.2 Infraestructura final

La renovación tecnológica de hardware y software que pretende el proyecto, buscará integrar todas y cada una de las funcionalidades soportadas por los sistemas actuales descritos en el punto anterior y ampliar las mismas, mejorando la seguridad en el acceso a los sistemas de información del Ayuntamiento, así como permitiendo una gestión y administración centralizada de los mismos y las alertas generadas asociadas.

Se requiere pues, la renovación tecnológica de todos los elementos indicados en el punto anterior que forman parte de la infraestructura de seguridad corporativa municipal. Por tanto, los oferentes deberán incluir en su propuesta el suministro, instalación y configuración de los siguientes elementos:

1. ***Sistema de cortafuegos perimetral en alta disponibilidad, con funcionalidades de nivel 7 (cortafuegos de nueva generación):***

   La oferta al presente pliego deberá incluir una pareja de cortafuegos de alta disponibilidad y con funcionalidades de nivel 7, que sustituya y complemente el comportamiento de la infraestructura actual de cortafuegos de seguridad perimetral. Estos cortafuegos tendrán que cumplir con los siguientes requisitos, además de incluir todas las funcionalidades de los equipos actuales:

   - Equipos cortafuegos de nueva generación en formato de *appliance* enracable.
   - Al menos 12 puertos RJ45 Gigabit Ethernet, para conexión a los distintos segmentos de red a separar.
   - Soporte para configuración de, al menos, 1000 políticas de control de acceso de nivel 7.

- Control dde aplicaciones y usuarios basada en políticas. Identificación de la aplicación independientemente del puerto, tipo de cifrado (SSL, TLS, SSH) o técnica evasiva empleada..
- Prevención de amenazas en tiempo real, detectando un amplio rango de *malware* y *exploits* de vulnerabilidades (virus, spyware, gusanos, etc) sin latencia, para todo tipo de amenazas.
- Protección contra ataques y pérdida de datos de las aplicaciones basadas en web y base de datos.
- Posibilidad de funcionamiento como sistema de detección y protección ante intrusiones IDP/IPS.
- Capacidades de servicio de VPN: IPSec (Site to Site y de usuarios) y túneles VPN SSL. Soporte de clientes VPN bajo plataformas Microsoft Windows, Mac OS, Android e IOS.
- Integración con Active Directory y LDAP para permitir identificar, controlar y aplicar reglas por usuario.
- Filtrado de URL basado en categorías actualizable y configurable así como funcionalidades de Proxy y Caché de contenidos para la navegación de usuarios.
- Bloqueo de amenazas como *Cross-site Scripting*, inyección SQL, desbordamiento de buffer, DoS y servicio de reputación de IP.
- Garantía por cada equipo de un *throughput* mínimo de 2Gb, con la identificación de aplicaciones habilitada y para todo el tráfico.
- Soporte de enrutamiento basado en políticas.
- Servicio de gestión de alertas e informes de seguridad integrable con solución de gestión centralizada.

2. ***Sistema de cortafuegos de segundo nivel para protección adicional de capa de servidores.***
   - Servicio de cortafuegos virtual que separa el acceso de usuarios a la red de servidores, así como proporciona una segunda capa en el acceso externo a dicha red.
   - Integrable en infraestructura de virtualización corporativa, basada en Vmware vsphere 5.5 Enterprise, con 4 hosts físicos de 2 procesadores hexacore.
   - Definición de reglas de control de acceso y de aplicaciones, con motor de clasificación de tráfico para detección y filtrado de ataques.
   - Integración con Active Directory y LDAP para permitir identificar, controlar y aplicar reglas por usuario.
   - Bloqueo de amenazas como *Cross-site Scripting*, inyección SQL, desbordamiento de buffer, DoS y servicio de reputación de IP.
   - Para este subsistema no se exigen requisitos de funcionamiento en cluster o alta disponibilidad del servicio.
   - Servicio de gestión a alertas e informes de seguridad, integrable con solución de gestión centralizada.

3. ***Sistema de seguridad de correo electrónico para la entrega y recepción de correo limpio de virus y spam***

   - Sistema de filtrado *antispam/antivirus* para entrega de correo limpio para 800 buzones de usuario. Estará integrado con la infraestructura de buzones de correo corporativos basada en el servidor de correo Zimbra
   - Entrega limpia de correo a servidor de buzones corporativo, con funciones de filtrado *antispam* por reputación y escaneo de virus.
   - Soporte de múltiples técnicas de detección de *spam*: técnicas de inspección de la conexión (reputación de origen, *botnets*, límite de conexiones...), técnicas de inspección de cabeceras (cumplimiento de RFCs, *greylisting*, listas blancas y negras...) y técnicas de inspección del contenido (heurístico, filtros bayesianos, filtrado de contenidos web, *newsletters*...).
   - El sistema propuesto deberá identificar y neutralizar amenazas específicas, como los ataques avanzados de *phishing*.
   - Posibilidad de definición de listas blancas y listas negras personalizadas.
   - Gestión de correo en cuarentena a nivel de usuario, integrada con *Active Directory* de Windows.
   - Servicio ofrecido en alta disponibilidad, garantizando la entrega de correo en modalidad 7x24x365.
   - Almacenamiento de correo en caso de caída del servidor de buzones interno.
   - Soporte de multiples dominios con posibilidad de configuraciones independientes para los dominios.
   - Servicio de gestión a alertas e informes de uso, integrable con solución de gestión centralizada.

4. ***Sistema centralizado de gestión de la infraestructura de seguridad, incluyendo control y correlación de eventos.***

   La nueva solución ofertada debe contemplar la gestión centralizada de todos los elementos de seguridad así como la centralización de los eventos de seguridad e informes de uso y alertas (reporting). La solución a implantar deberá cumplir las siguientes características:

   - Inclusión de gráficas predefinidas y personalizables para monitorizar, identificar y alertar contra distintos patrones de ataque.
   - Incorporación del módulo de correlación de eventos de seguridad de los distintos subsistemas incluidos, permitiendo la alerta temprana e identificación de posibles vulnerabilidades y amenazas.
   - Almacenamiento necesario para albergar la información de registros de todos los componentes de al menos dos meses de antigüedad
   - Se valorará la inclusión de herramientas de análisis forense para la explotación y auditoría de los registros de eventos almacenados.

Los requisitos que deberá cumplir la infraestructura suministrada para la gestión centralizada y de informes de alertas se detalla más adelante, en el punto 5 del presente documento.

Para todos los sistemas nuevos a incorporar, será requisito indispensable la integración de toda la nueva plataforma, dentro de los siguientes entornos:

- Integración con la infraestructura de red multiservicio existente en la actualidad en el Ayuntamiento, así como con la arquitectura de servidores de dominio basados en Active Directory de Windows.
- Integración con la red SARA que permita acceder a los servicios publicados desde otras administrativas incidiendo así en la mejora de movilidad ciudadana y en el ahorro de costes directos a las administraciones.
- Integración con operadores que actualmente ofrecen el servicio de conexión a Internet en las dependencias municipales para garantizar, tanto el acceso ciudadano con la mayor disponibilidad posible a los servicios de administración electrónica publicados y a publicar, como a los empleados a conectarse a los distintos servicios publicados.
- Exigencia de inclusión en la oferta del contratista de cualquier elemento extra necesario para el conexionado de la nueva infraestructura para conseguir la nueva arquitectura de seguridad ofertada (cableado, electrónica de red, conectores de fibra, etc).

3.3 Requisitos funcionales a cumplir

El suministro de la nueva infraestructura de seguridad demandado en el punto anterior deberá cubrir y ampliar las capacidades realizadas por la infraestructura actual y deberá aportar todas y cada una de las siguientes funcionalidades:

- Control de tráfico de aplicación entre las distintas redes a securizar (DMZ, red de servidores, redes de acceso).
- Doble capa de seguridad y control de acceso para red de servidores.
- Terminación de túneles VPN IPSec para conexión a red interadministrativa, VPN corporativa de usuarios y otras posibles conexiones *site to site*. Soporte de clientes VPN bajo plataformas Microsoft Windows, Mac OS, Android e IOS.
- Control de navegación por usuario
- Servicio de filtrado de URL basado en categorías, proxy y caching de contenidos para navegación de empleados municipales.
- Administración centralizada de toda la infraestructura de seguridad desplegada.
- Gestión centralizada de informes y alertas de seguridad con posibilidad de incorporación de herramientas de correlación de eventos y análisis forense.

El oferente incluirá en su propuesta una tabla matriz en la que se detalle el cumplimiento de las funcionalidades enumeradas en este punto por cada uno de los sistemas a incorporar como renovación tecnológica de la infraestructura de seguridad, así como cualquier otra funcionalidad extra de seguridad aportada que considere de interés.

La siguiente figura muestra un ejemplo de cómo debe formularse dicha tabla:

Funcionalidad exigida	*Sistema implicado*	*Descripción operativa*
Control de navegación por usuario	Cortafuegos perimetral	Mediante reglas de acceso a navegación web integradas con Directorio Activo/LDAP

3.4 Plan de migración

El adjudicatario del presente concurso será responsable del despliegue de toda la nueva infraestructura suministrada y la adecuación de la misma para el cumplimiento de todas las funcionalidades demandadas, migrando las capacidades de los sistemas actuales en la nueva solución implantada.

Las empresas que deseen concurrir al presente pliego deberán incluir en su oferta un detallado plan de migración que recoja los pasos necesarios para permitir el paso de la situación actual descrita a la infraestructura final demandada, incluyendo la adaptación de los nuevos elementos a las políticas actuales existentes, así como configurando los elementos para mantener las conexiones VPN existentes.

Dicho plan deberá ser posteriormente consensuado con el personal técnico municipal y deberá incluir la siguiente documentación:

- Descripción y diseño de red de la solución final conjunta propuesta.
- Planificación temporal estimada y descripción de las tareas.
- Equipo técnico asignado, responsable de cada una de las tareas y fases.
- Ventanas de actuación para cambios e incidencias sobre el trabajo diario de los empleados municipales.
- Posibles riesgos y/o contingencias.
- Descripción de pruebas de funcionalidad y operativa.

3.5 Requisitos de documentación

Las empresas contratistas que opten a la ejecución del presente pliego deberán presentar en su oferta, como mínimo, la documentación que se indica a continuación, detallando la solución técnica de la plataforma suministrada, junto con las condiciones de soporte y mantenimiento ofrecidas. En caso de resultar adjudicatarias, dicha documentación será revisada conjuntamente con el personal técnico municipal para incluir mayor detalle de cara a la ejecución del proyecto en el plazo de un mes posterior a la adjudicación del contrato.

Deberán incluirse como mínimo en la propuesta los siguientes documentos:

- Descripción técnica de la solución con detalle de la arquitectura resultante así como los elementos hardware y software ofertados.
- Plan de migración, según lo descrito en el punto anterior.
- Plan de pruebas. Detalle de pruebas unitarias de cada uno de los elementos incluidos y pruebas de integración dentro de la red corporativa municipal de los distintos subsistemas de seguridad.
- Plan de mantenimiento. Según lo indicado en el punto 4 del presente documento.

3.6 Requisitos legales

La ejecución del presente proyecto vendrá enmarcada dentro de la normativa establecida para las Administraciones públicas en materia de Administración Electrónica, Seguridad e Interoperabilidad, teniendo presente especialmente las normativas siguientes:

Ley 11/2007, de 22 de junio, de Acceso electrónico de los ciudadanos a los Servicios Públicos. BOE núm. 150 de 23/06/2007

Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 3/2010, de 8 de enero, determina la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos

El Esquema Nacional de Interoperabilidad (ENI), regulado por el Real Decreto 4/2010, de 8 de enero, establece el conjunto de criterios y recomendaciones que deberán ser tenidos en cuenta por las AAPP para la toma de decisiones tecnológicas que garanticen la interoperabilidad.

4 DESCRIPCIÓN DEL SERVICIO DE MANTENIMIENTO Y SOPORTE DEMANDADO

El adjudicatario garantizará que todos los componentes de la instalación estén en **perfecto estado de conservación y funcionamiento** durante la vigencia del contrato. En las condiciones contractuales se incluyen:

- Soporte técnico.
- Mantenimiento correctivo.
- Mantenimiento preventivo.
- Averías por causas externas a la instalación.
- Documentación y partes de trabajo.

En todo momento, la empresa contratista deberá *hacerse cargo del coste de las licencias de todo el hardware y software activo durante la vigencia del contrato resultante de las adquisiciones necesarias para el cumplimiento de los requisitos de seguridad demandados así como de aquellas renovaciones de licenciamiento de la infraestructura existente en caso de que el contratista lo considerara necesario para el cumplimiento del pliego. El oferente incluirá en este punto detalle de los costes derivados de dicho licenciamiento durante los años de duración de la prestación del servicio.*

Aquellas tareas no recogidas dentro del marco de mantenimiento de la instalación, pero relacionadas con cualquier cambio, adaptación o mejora de la misma, serán facturadas aparte por la empresa adjudicataria. Para ello, debe ser adjuntada al presente contrato la correspondiente baremación económica que recoja de forma detallada el coste por hora de cada tipo de tarea a contemplar, rellenando la tabla que se adjunta en el Anexo 3 del presente documento.

Las empresas que opten a este contrato deberán demostrar con la documentación correspondiente (ver Pliego de Prescripciones Administrativas) tener la capacidad y conocimientos necesarios para operar, administrar y mantener toda la infraestructura de telefonía fija corporativa recogida en este pliego.

4.1 Soporte técnico.

El contratista prestará un servicio de atención y soporte técnico al Ayuntamiento mediante teléfono y correo electrónico o portal de incidencias. El horario de prestación de este servicio será de lunes a viernes no festivos de 9:00 h a 14:00 h por la mañana, y de 16:00 h a 19:00 h por la tarde. Este mismo servicio se hará cargo de la notificación de incidencias.

Para la notificación de incidencias fuera de este horario el contratista pondrá a disposición del presente contrato una centralita con servicio las 24 horas del día todos los días del año así como un servicio de gestión de incidencias mediante buzón de correo electrónico y/o aplicación de gestión de incidencias.

El alcance de los servicios de administración y mantenimiento de la propuesta deberá comprender lo siguiente:

- Sustitución de elementos hardware averiados por otros de iguales o mayores prestaciones, incluyéndose la mano de obra y desplazamientos de los técnicos especializados que sea necesarios.

- **Telemantenimiento de los sistemas** según los requisitos del presente pliego, para lo que el Ayuntamiento facilitará conexión a los mismos a la empresa adjudicataria.

- **Mantenimiento preventivo**, planificando y realizando actividades de inspección preventiva y puesta a punto para minimizar la incidencia de posibles averías en el sistema. Como parte del mantenimiento preventivo, el oferente mantendrá copias de seguridad de las configuraciones y bases de datos de los sistemas con la periodicidad adecuada para evitar pérdidas de información y garantizar una rápida restauración de los sistemas, en caso de avería grave.

- **Actualizaciones de versiones/revisiones** menores o mayores orientadas a garantizar la estabilidad del sistema.

- **Soporte técnico para consultas referentes a la explotación del sistema**, en particular en lo relativo a la gestión y administración del software de la plataforma de forma que se garantice el acceso al mismo por el personal técnico del Ayuntamiento habilitado para tareas de gestión, configuración y administración básicas.

- **Cambios en la configuración del sistema** sobre las funcionalidades implantadas en la fase de instalación y puesta en marcha. El adjudicatario incluirá detalle de trabajos de configuración y adaptación incluidos en el mantenimiento, así como aquéllos que impliquen un coste al Ayuntamiento. En el Anexo 3 del presente documento pueden consultarse las tareas mínimas de configuración que deben ser incluidas por el adjudicatario dentro del servicio de mantenimiento.

4.2 Mantenimiento correctivo.

La empresa adjudicataria del contrato se responsabilizará en todo momento del diagnóstico y mantenimiento correctivo de los diferentes elementos que forman parte del sistema de seguridad perimetral resultante de la ejecución del contrato. Una incidencia o avería incluye cualquier evento que no es parte de la operación normal de un servicio y que causa, o puede causar, una interrupción o degradación de la calidad de dicho servicio.

Las actividades de mantenimiento correctivo consisten en la identificación de la avería, resolución de incidencias y reparación de los dispositivos que sea preciso, con el fin de disminuir la indisponibilidad de equipos por causa de avería o incidencia en los mismos.

Para la resolución de averías se establecerá un sistema de escalado y priorización, basado en la gravedad de los incidentes. Este escalado alcanzará a todos los perfiles profesionales ofertados por el contratista e incluso a personal experto del fabricante de los equipos.

El mantenimiento correctivo se realizará, tanto en la ubicación del equipo a reparar (***in situ***), como en el taller o laboratorio habilitado para ello, consistiendo en reparar los subconjuntos o en efectuar ajustes de piezas.

Las etapas principales de una intervención serán las siguientes:

- Recepción del aviso de avería en el centro de mantenimiento.
- Aceptación del aviso de avería.
- Confirmación de la avería.
- Identificación de la causa.
- Arreglo mediante acciones simples.
- Cambio de material si el arreglo no es posible.
- Verificación del funcionamiento.
- Notificación al Ayuntamiento.

Con el fin de dar cumplimiento a los tiempos de reparación, los técnicos encargados dispondrán de toda la información necesaria para ello, tanto de conocimiento del equipo, manuales de fabricante, etc., como procedimientos de actuación y flujos de trabajo.

Prioridad de las averías

Se diferenciarán los siguientes tipos de prioridades para las incidencias producidas:

- Prioridad 0 / Emergencia: Indisponibilidad completa del sistema, quedando el mismo totalmente fuera de producción/funcionamiento.
- Prioridad 1: el sistema se encuentra gravemente degradado y, por tanto, la producción/funcionamiento está interrumpida en una parte importante.
- Prioridad 2: el sistema pierde parcialmente su capacidad en alguna de sus funcionalidades, debido a problemas, que de no ser tratados de inmediato, pueden escalar a problemas de mayor prioridad con afectación de servicio.
- Prioridad 3: el sistema funciona de forma correcta y sin peligro de degenerar en pérdida de servicio, pero existen aspectos secundarios o de acabado a corregir.

Tipos de perfiles profesionales

Para la resolución de incidencias, el adjudicatario contará con diversos perfiles profesionales, que debe detallar cuantitativa y cualitativamente en su oferta. Estos perfiles serán de los siguientes tipos:

- Perfil Nivel 1: Se trata de aquel perfil que realiza tareas básicas, fundamentalmente a nivel de hardware, resolución de incidencias, reparaciones electrónicas y realización de instalaciones. Equivale a un técnico superior en sistemas de telecomunicación, electrónicos e informáticos.
- Perfil Nivel 2: Se trata de aquel perfil que realiza tareas avanzadas, a nivel hardware y software, tareas de configuración y gestión de sistemas de comunicaciones y electrónica, coordinación de grupos de los medios humanos, etc. Equivale a un ingeniero de grado medio con conocimientos similares a los del perfil nivel 1, añadiendo gestión de sistemas y mantenimiento evolutivo de sistemas.
- Perfil Nivel 3: Se trata de aquel perfil de soporte experto, también denominado de alto nivel, con capacidad para diagnosticar un problema que haya surgido en el sistema y desarrollar un plan de acción adecuado para solventar dicho problema.

Tiempos de asistencia *in situ*

Tiempo de localización: Inmediato

Tiempo de resolución:

Prioridad de la avería	Tiempo de resolución
Prioridad 0 / Emergencia	4 horas
Prioridad 1	4 horas
Prioridad 2	8 horas
Prioridad 3	24 horas

4.3 Mantenimiento preventivo.

Las operaciones de mantenimiento preventivo tendrán como finalidad minimizar la aparición de averías en el sistema. Con ello se intenta disminuir el número de acciones correctivas, mejorando sensiblemente la disponibilidad de la infraestructura.

Las operaciones de mantenimiento preventivo se efectuarán principalmente de forma periódica (programada mensual, trimestral o anualmente) o en función de las alarmas y defectos menores detectados.

Las empresas oferentes deberán detallar el tipo de tareas que llevarán a cabo, dentro del marco del mantenimiento preventivo, para conseguir mantener la infraestructura en un estado óptimo y con el fin de conseguir minimizar el número de incidencias ocasionadas.

Entre las tareas de mantenimiento preventivo, aparte de otras que el oferente pudiera considerar necesarias, deberán incluirse como imprescindibles las indicadas en la tabla siguiente:

Tareas de mantenimiento preventivo básicas a incluir	
TAREA	**PERIODICIDAD**
Monitorización y supervisión de equipos para alerta temprana	Diaria
Gestión de copias de seguridad de configuración y bases de datos	Semanal
Rotación de log y borrado de datos antiguos (faxes, grabaciones, etc)	Mensual
Revisión del estado de elementos hardware	Mensual
Medidas de calidad de los servicios	Trimestral
Inventario y documentación de recursos	Anual

El oferente deberá incluir en su propuesta estas tareas, así como aquéllas que considere puedan ser de interés para el Ayuntamiento, para ser valoradas en el proceso de adjudicación del contrato.

4.4 Averías por causas externas a la instalación

Cuando se produzca una **avería por causas externas a la instalación,** como uso indebido, inundaciones en las salas técnicas o cualquier otra inclemencia meteorológica y, en general, cualquier causa que sea ajena a sus condiciones de funcionamiento y a la actuación del adjudicatario, si es procedente, la reparación será ordenada por los Servicios Técnicos Municipales y será ejecutada por el adjudicatario.

Si la avería es relativamente importante, se podrá acordar la sustitución del elemento por otro nuevo. En caso de que el coste de estas reparaciones sea asumido por el adjudicatario, que posteriormente se encargará de reclamar a los causantes de los daños el correspondiente resarcimiento económico de los costes sufridos.

4.5 Documentación y partes de trabajo.

Con periodicidad mínima mensual, el adjudicatario presentará ante los Servicios Técnicos del Ayuntamiento el parte de actuaciones que hayan tenido lugar, ya sean de mantenimiento preventivo o correctivo, así como la posible documentación asociada.

Este parte, tendrá como mínimo los siguientes campos:

- Fecha del aviso
- Notificación del aviso
- Número de aviso
- Clase o tipo de aviso
- Hora de recepción del aviso
- Lugar del aviso
- Hora de comunicación al operario o al equipo de actuación
- Hora de llegada del equipo al lugar de la incidencia
- Identificación del equipo u operario que realizó la reparación
- Clase de avería
- Materiales empleados en la reparación
- Incidencias generales en la avería y su reparación

A su vez, el adjudicatario deberá adjuntar en cada intervención in situ la correspondiente hoja de informe de trabajos detallando el personal empleado, las horas necesitadas para la subsanación del problema así como cualquier material que hubiera sido necesario reemplazar. Estas hojas de informe tendrán un formato estándar reconocible y deberán ser firmadas y aprobadas por personal del Ayuntamiento a la finalización de los trabajos.

5 REQUISITOS PARA LA GESTIÓN CENTRALIZADA DE LA INFRAESTRUCTURA DE SEGURIDAD

Además de la renovación tecnológica y el mantenimiento de las nuevas infraestructuras ofertadas, el adjudicatario deberá facilitar un sistema que simplifique la gestión de la seguridad de forma centralizada, con herramientas de gestión de los registros de los distintos elementos que permita la detección temprana de amenazas y la correlación de eventos entre las distintas plataformas de seguridad implantada.

La empresa facilitará una solución SIEM que implemente, al menos, las siguientes características de este tipo de soluciones:

- Permitir el control y gestión simplificada de todos los elementos de la infraestructura de seguridad, desplegada a través de una consola unificada, con conexión a todos los módulos necesarios para la operación de cada una de las plataformas.
- Recolectar la información
- Capacidad de gestión de logs con fines de auditoría forense.
- Soportar la ampliación de la capacidad de la plataforma para la incorporación de nuevos módulos de gestión de otras infraestructuras así como la recolección de eventos de seguridad generados por las mismas.

6 EQUIPO Y PLAN DE TRABAJO

Para el desarrollo del proyecto y su implantación se requiere la constitución de un equipo de trabajo que realizará las tareas planificadas con antelación bajo la supervisión del personal municipal responsable de la administración de la red y seguridad en lo sistemas de información del Ayuntamiento.

6.1 Equipo de trabajo

El equipo de trabajo para la ejecución del proyecto estará compuesto por un mínimo de tres personas con los requisitos mínimos asociados a los siguientes perfiles:

- *Jefe de proyecto/responsable del servicio*: realizará el seguimiento y supervisión de la implantación del proyecto conjuntamente con el personal municipal que se asigne al mismo. Se encargará con el resto de su equipo de la toma de datos inicial y planificación de todas la tareas y personal a su cargo.
- *Técnico Senior de redes y seguridad*: se encargará de la definición de la solución y configuración avanzada de la misma así como de la formación del personal municipal.
- *Técnico Junior de redes y seguridad*: se encargará de la instalación básica del equipamiento y las pruebas de funcionamiento conjuntamente con el personal municipal asignado a las mismas.

6.2 Planificación

La empresa encargada de la ejecución del proyecto presentará una planificación detallada de los trabajos necesarios para la implantación de cada una de las infraestructuras de seguridad demandadas, poniendo especial detalle en el procedimiento de migración

Es recomendable una planificación separada y en detalle de la implantación de cada uno de los distintos sistemas de seguridad a migrar para minimizar el impacto en la indisponibilidad de los servicios como resultado de los cambios en las infraestructuras de seguridad a mejorar.

7 FORMACIÓN

Una vez finalizados y configurados los nuevos sistemas objeto del proyecto, se llevará a cabo un plan de formación sobre la solución implantada, para la correcta explotación, mantenimiento y cambios de configuración, para el personal técnico municipal implicado en el proyecto responsable de la explotación de la infraestructura resultante.

La formación será impartida, en cualquier caso, en las dependencias del Ayuntamiento y deberá cubrir los aspectos más importantes de los equipos y de la tecnología implantada, determinándose el calendario de las sesiones, así como los asistentes, de forma consensuada entre el personal del Ayuntamiento y el licitador.

A continuación se detallan los diferentes cursos de formación que, como mínimo, será necesario impartir:

- Formación técnica en administración y configuración de los sistemas de seguridad perimetral implantados.
- Formación técnica en administración y gestión de los sistemas de seguridad en el servicio de correo que se implanten.
- Formación técnica en el uso y mantenimiento de cualquier software adicional incluido con la solución (gestión de registros, gestión de alertas, etc)

- Formación en el uso del servicio de asistencia de soporte y mantenimiento ofertado por la empresa adjudicataria del contrato.

Las empresas que concurran al concurso deberán presentar en su oferta una versión tentativa de dicho plan de formación indicando los cursos a incluir, horas de formación y número de asistentes para cada uno de ellos. El calendario de la formación será consensuado conjuntamente con el personal del Ayuntamiento, tomando como base dicha planificación tentativa.

8 TRANSFERENCIA TECNOLÓGICA

Durante la duración del servicio objeto del contrato, el adjudicatario deberá facilitar en todo momento al personal designado por el Ayuntamiento para la supervisión del servicio, toda aquella información y documentación que soliciten para tener el conocimiento del estado de la infraestructura, así como de las circunstancias y condiciones en las que se desarrolla el mismo y posibles problemas puntuales que puedan presentarse, junto con las tecnologías, procedimientos y herramientas empleados para resolverlos.

En particular, el contratista contará en todo momento con documentación actualizada de la configuración, registros de incidencias, mapa de red e inventario de la infraestructura, así como los procedimientos de mantenimiento llevados a cabo para garantizar el correcto funcionamiento y estado óptimo de toda la infraestructura de seguridad objeto del soporte debiendo facilitar dicha documentación al personal técnico designado por el Ayuntamiento, al menos con una periodicidad semestral, pudiendo ser demandada en cualquier otro momento, por necesidades del servicio.

Cuando finalice el contrato, el adjudicatario estará obligado a facilitar de forma detallada todo el conocimiento y documentación necesaria para permitir la correcta prestación del servicio. Para ello, deberá presentar 2 meses antes de la finalización del mismo documento de cesión del servicio que describa detalladamente, el estado de todos los sistemas objeto del mantenimiento con sus configuraciones, condiciones de acceso, etc.

9 ANEXOS

ANEXO1: DETALLES DE EQUIPAMIENTO Y LICENCIAMIENTOS EXISTENTES

9.1 Cortafuegos perimetrales Stonegate

Número de serie	Descripción Equipo	Características
VM-120103-08-14	Firewall de nivel 4 McAffee Stonesoft 1030	▪ Formato Appliance entrañable en 1 U ▪ 6 puertos Gigabit Ethernet ▪ 1 Gbps de througput y 700000 conexiones concurrentes sin inspección ▪ Consola centralizada McAffee Security Management Center 5.7.4 ▪ Ver detalles de licenciamiento en figura al final del cuadro
VM-120918-01-01	Firewall de nivel 4 McAffee Stonesoft 1030	▪ Formato Appliance entrañable en 1 U ▪ 6 puertos Gigabit Ethernet ▪ 1 Gbps de througput y 700000 conexiones concurrentes sin inspección ▪ Consola centralizada McAffee Security Management Center 5.7.4 ▪ Ver detalles de licenciamiento en figura al final del cuadro

Name	Status	Bound To	Binding	Version	Expires	Maintenance Contract Expires	Support Level	Allocated To
Management Server License (1 element)								
Management Server (static license)	Bound	Management192.168.1.136		6.0		2016-09-28 23:59:59.0	Active	Shared Dom
Log Server License (1 element)								
Log Server (static license)	Bound	Log Server 192.168.1.136		6.0		2016-09-28 23:59:59.0	Active	Shared Dom
Firewall Node License (2 elements)								
Firewall Node (dynamic license)	Bound	ayto29ocsi0c53c5-2dae3-142b9-cc14e		5.8		2016-09-28 23:59:59.0	Active	Shared Dom
Firewall Node (dynamic license)	Bound	ayto29ocsi0 c53c5-2dae3-142b9-cc14e		5.8		2016-09-28 23:59:59.0	Active	Shared Dom

9.2 Cortafuegos de aplicación con filtrado web Sonicwall

Número de serie	Descripción Equipo	Características
0017C5B07CA4	Equipo Primario Firewall de nivel de aplicación Sonicwall NSA 240 Expanded	▪ 3 puertos Gigabit Ethernet ▪ 5 puertos 100Mbps Ethernet ▪ Ver resto de características y licenciamento en siguiente figura
0017C5679934	Equipo Primario Firewall de nivel de aplicación Sonicwall NSA 240 Expanded	▪ 3 puertos Gigabit Ethernet ▪ 5 puertos 100Mbps Ethernet ▪ Ver resto de características y licenciamento en siguiente figura

Model:	NSA 240 Expanded
Product Code:	6981
Serial Number:	0017C5B07CA4
Authentication Code:	5HLS-AW5Y
Firmware Version:	SonicOS Enhanced 5.8.1.4-43o
Safemode Version:	SafeMode 5.0.1.13
ROM Version:	SonicROM 5.0.2.12
CPUs:	23.94% - 2 x 500 MHz Mips64 Octeon Processor
Total Memory:	256 MB RAM, 32 MB Flash
System Time:	08/12/2016 14:39:12
Up Time:	12 Days 06:08:53
Connections:	Peak: 8081 Current: 3129 Max: 13125
Connection Usage:	23.840

Service Name	Status
Nodes/Users	Licensed - Unlimited Nodes
SSL VPN Nodes/Users	Licensed 2 Nodes (0 in use)
VPN	Licensed
Global VPN Client	Licensed - 2 Licenses (0 in use)
CFS (Content Filter)	Licensed
McAfee AV Enforcement	Not Licensed
Gateway Anti-Virus	Licensed
Anti-Spyware	Licensed
Intrusion Prevention	Licensed
App Control	Licensed
App Visualization	Licensed
Anti-Spam	Not Licensed
ViewPoint	Licensed
DPI-SSL	Not Licensed
WAN Acceleration Software	Not Licensed
Botnet	Licensed

9.3 Equipo de seguridad para correo Antispam/Antivirus Ironport

Número de serie	Descripción Equipo	Características
30F70D47CFFB-FGL1641403P	Cisco Email Security (Ionport C170)	▪ Formato appliance enracable en 1 U ▪ 2 puertos Gigabit Ethernet ▪ Procesador dual core 2,8GHz y 4 Gb de RAM ▪ Ver licenciamiento en figura al final del cuadro
30F70D47CFEC-FGL1641403Z	Cisco Email Security (Ionport C170)	▪ Formato appliance enracable en 1 U ▪ 2 puertos Gigabit Ethernet ▪ Procesador dual core 2,8GHz y 4 Gb de RAM ▪ Ver licenciamiento en figura al final del cuadro

Description	Status	Time Remaining	Expiration Date
Centralized Management	Active	162 days	21 Jan 2017 15:08 (GMT +01:00)
IronPort Email Encryption	Dormant	30 days	N/A
IronPort Anti-Spam	Active	162 days	21 Jan 2017 15:08 (GMT +01:00)
Sophos Anti-Virus	Active	162 days	21 Jan 2017 15:08 (GMT +01:00)
Bounce Verification	Active	Perpetual	N/A
Incoming Mail Handling	Active	Perpetual	N/A
Outbreak Filters	Active	162 days	21 Jan 2017 15:08 (GMT +01:00)

C.I.F.: P-2813400-E