Zaragoza
AYUNTAMIENTO

DIRECCIÓN GENERAL DE CIENCIA Y TECNOLOGÍA
SERVICIO DE REDES Y SISTEMAS

Pliego de Condiciones Técnicas del contrato de suministro de licencias de uso y soporte de diversas herramientas de seguridad como infraestructura de los Sistemas de Información Corporativos.

1 OBJETIVO

El Ayuntamiento de Zaragoza dispone en la actualidad de una gran red datos que interconecta mas de 3.400 ordenadores de usuarios y 100 servidores.
A disposición de todos ellos se encuentra la conexión corporativa a Internet (24x7), que permite navegar por la red y hacer uso del correo electrónico con entrada y salida a Internet, del que disponen todos los trabajadores municipales. Ambos servicios se consideran imprescindibles para el trabajo diario. Poner estas herramientas a disposición de toda la red municipal, implica un gran riesgo de seguridad que requiere soluciones que permitan controlar y minimizar los problemas derivados de virus, troyanos, spam, malware y todo tipo de amenazas que circulan por la red, cuyas consecuencias, como la parada de servicio, la pérdida de datos y el robo o manipulación de información pueden ser catastróficas.

Una de las amenazas imprescindibles de controlar son los virus, que circulan constantemente por la red, por lo tanto una de las herramientas imprescindibles son las conocidas como antivirus ó antimalware. El Ayuntamiento dispone de licencias de uso de estas herramientas que distribuye entre todas sus máquinas.

Con objeto de seguir garantizando la seguridad mínima en la prestación de los servicios de red del Ayuntamiento de Zaragoza es imprescindible la renovación de las licencias de uso y el soporte de sistemas antivirus corporativos para la protección básica del entorno informático municipal, tanto en el ámbito del PC de escritorio (Desktop con Windows y Linux) como el de servidores (multiplataforma Netware, Linux y Windows), todo ello con sistema de Gestión y Políticas de Seguridad Centralizadas (ePolicy).

Por otra parte es necesario disponer de soluciones integradas de seguridad de contenidos, tanto web como de mensajería que prevenga del riesgo de fuga de la información municipal reservada.

Para gestionar el ancho de banda y realizar un filtrado de contenidos es necesario disponer de una tecnología de filtrado de contenidos, que evite el abuso en los accesos a Internet provocado por usuarios accediendo a contenidos no apropiados, o usuarios que descargan de gran tamaño, juegos, música, etc. que limita la capacidad de la red para dar un servicio adecuado a la gestión diaria.

Otra de las necesidades que se pretende cubrir con este contrato menor es la de proporcionar una extensa cobertura de seguridad en la protección del servidor de correo: Anti-Spam, Anti-Virus, Anti-Relay, Hacker Prof, Backscatter, resistencia a bombardeo de correo,IP reputation,Sistema anti Zombie(ZDS), asegurando el mantenimiento y gestión de mensajes en cuarentena, por usuario y recogida automatizada mediante mensajes. La existencia registro de logs unificado que permita analizar y resolver incidencias de correo de forma rápida y eficiente.

Por último se debe disponer de una solución SSL VPN para el despliegue de conexiones seguras desde Internet a la red municipal, permitiendo el despliegue de servicios tales como el telemantenimiento remoto especializado, el despliegue de una extranet municipal y la puesta en marcha segura del teletrabajo del empleado municipal.

2 Objeto del Contrato:

Seguir garantizando la seguridad mínima y la prestación de los servicios de red del Ayuntamiento de Zaragoza, para lo que es imprescindible la renovación de las licencias de uso y su soporte de, entre otros, los sistemas antivirus corporativos, securización de contenidos municipales, mejora en el rendimiento de aplicaciones críticas de la red municipal, y la gestión de la red de invitados y sus contenidos, para la protección básica del entorno informático municipal.

3 Requisitos técnicos

3.4 Requisitos software

El presente contrato debe contemplar la renovación de los siguientes elementos del equipamiento informático municipal:

1. Quinientas una (501) licencias de uso de McAfee Active Virus Defense para Gobierno (2 Yr GL P++) distribuidas en 250 licencias para Linux y 251 para Windows .

2. Renovación de 25 Licencias de uso de la herramienta Websense. (network user) licencia municipal : DQ9CC43U394RBNFU,

3. 1 Licencia de uso de la herramienta SurfControl referencia NS-WF-ssg5-R : subscription renewal for Web Filtering on SSG5

4. Licencias de Pineapp: Mail-SeCure 3010 1Y y Always Secure PA-MAIN-3010

5. Licencias Infoblox renovación ed mto (DNS, DHCP, GRID) de 2 maquinas IB -550 (serial number: 1006200704000005 y 1006200806000013, HW id: 29b2c77e1d25682658f6262555391, f8e1ec5ec863390aa257b5c6a613b1b)

6. Quinientas (500) licencias de Sophos Pure Message AV/AS/EP (Email Security & Data Protection, programa Gobierno), incluyendo :

- - Pure Message for Unix / Linux
- - Email protection (Antivirus, antispam)
- - Email Policy
- - SAV Interface

7. Mantenimiento para el appliance de seguridad (VPN-SSL) Juniper SA2000, hasta 100 usuarios simultáneos.

4 Requisitos de Soporte

La propuesta debe incluir el servicio de soporte y mantenimiento a incidencias del entorno con las siguientes condiciones:

- El tiempo de atención para comunicación de incidencias será de un mínimo de 9 horas al día, de 09:00 a 18:00h, de lunes a viernes laborables.
- Se ofrecerá un mecanismo de apertura de incidencias con al menos estos tres tipos de forma contacto: telefónico, por web y por e-mail.
- El tiempo de respuesta máximo tras la comunicación de una incidencia abierta dentro del horario de atención será de 60 minutos.
- Se proporcionará una herramienta de seguimiento de las incidencias
- El contrato de soporte incluirá
  - ✔ La reparación o sustitución de los elementos referidos en caso de avería, con un tiempo máximo de reposición de 4 días desde la comunicación de la avería.
  - ✔ La solución de incidencias en el software de los equipos y la actualizaciones de software que se requieran.
  - ✔ La solución de incidencias que afecten a la funcionalidad del entorno.

- Se tendrá acceso a servicios de soporte ofrecidos directamente por el fabricante.
- La empresa adjudicataria no dejará incidencias abiertas sin dar respuesta a las mismas por un tiempo superior a 24 horas.

La empresa adjudicataria enviará la documentación correspondiente al Servicio de Redes y Sistemas el día siguiente a la firma del contrato:

- Certificado de inicio de los servicios del fabricante
- Información de soporte online
- Información de soporte telefónico
- Procedimientos de apertura y gestión de incidencias.

Zaragoza 3 de Octubre de 2012

Jorge Calvera Lafuente
Técnico Superior de Sistemas

Alberto Virto Medina
Jefe de Servicio de Redes y Sistemas