PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HA DE REGIR EL CONTRATO DE SUMINISTRO DE LICENCIAS DE UN ANTIVIRUS CORPORATIVO PARA EL AYUNTAMIENTO DE SAN SEBASTIÁN DE LOS REYES

Fdo. Tomás Sanz Romero
Técnico de Sistemas

Fdo. Fernando Prats Sevilla
Jefe de Sección de Sistemas de Información

V°B°

Fdo. Alicia Herrero Fernández
Jefa de Servicio de Nuevas Tecnologías y Procesos

Índice

1. OBJETO DEL CONTRATO.

Este contrato tiene por objeto el **suministro de licencias** para la protección contra software malicioso (virus/malware, spyware, etc.) en la plataforma informática del Ayuntamiento de San Sebastián de los Reyes (en adelante el Ayuntamiento): puestos de trabajo cliente (disco, memoria, sistema operativo, navegación, correo electrónico, dispositivos extraíbles), portátiles, clientes ligeros VDI, servidores Windows tanto físicos como virtualizados y sistemas de almacenamiento.

El número de licencias necesarias debe cubrir el parque informático especificado en el Anexo I (apartado 5 del presente pliego).

2. ANTIVIRUS CORPORATIVO ACTUAL.

Actualmente el Ayuntamiento cuenta como solución antimalware (sobre Sistema Operativo Windows) con:

- Panda Antivirus para 651 puestos de trabajo y 22 servidores.
- Karspersky para 19 puestos de trabajo.

Como solución Antispam se utilizan dos *appliances* IronPort con la última versión de software instalada y renovada hasta noviembre de 2015. En cuanto a la navegación web corporativa, se utilizan dos equipos Sonicwall que realizan filtrado de categorías de páginas web (URLs), con soporte hasta agosto de 2015.

Todos los puestos de trabajo se encuentran conectados a la red corporativa municipal, lo que facilita las tareas de desinstalación, instalación, actualización y mantenimiento de todo el parque informático de forma centralizada. Tan sólo en algunos casos puntuales se cuenta con PCs fuera de dicha red, cuyo antivirus también debe ser actualizado.

3. ANTIVIRUS CORPORATIVO PROPUESTO.

Se deberán cumplir todas y cada una de las características técnicas descritas en los epígrafes siguientes:

3.1 ALCANCE.

Con el objeto de renovar los mecanismos de protección antimalware (antivirus corporativo) en los equipos informáticos del Ayuntamiento, se utilizará una solución modular de software comercial, conformada por varios componentes dedicados a la protección de los sistemas relacionados en el Anexo I, permitiéndose la instalación de agentes individuales en los mismos.

En la oferta correspondiente vendrán detallados todos los componentes de la solución, los cuales deberán poderse controlar conjuntamente mediante una herramienta software de consola central que actúe como punto único de gestión.

Dicho servicio (consola de gestión) se podrá ofrecer en modalidad *Cloud*, siempre y cuando se garanticen totalmente las opciones de disponibilidad, accesibilidad, seguridad, actualización, etc.

La consola central deberá estar accesible para los técnicos municipales, pudiéndose definir diferentes perfiles de acceso para los mismos, con el fin de poder llevar a cabo tareas de instalación de los productos en equipos remotos, actualizaciones periódicas, análisis de equipos, informes, auditoría y explotación de información de actividad (*logs*), resolución de incidencias, etc.

El adjudicatario será responsable de realizar la implantación de la solución antimalware, desinstalando la actual. Deberá incluirse el despliegue de los agentes antivirus en todos las máquinas del Ayuntamiento.

3.1 CARACTERÍSTICAS GENERALES.

La solución antimalware hará uso de una red global de inteligencia, accesible a través de Internet, con información constantemente actualizada (base de datos de inteligencia de seguridad), mantenida por el fabricante y accesible en tiempo real, sobre al menos:

- Patrones de firma antimalware.
- Patrones de firma antispyware.
- Reputación de archivos: Mediante lista de archivos con clasificación de reputación que refleje la probabilidad de que el archivo en cuestión sea malware.
- Nuevas vulnerabilidades que vayan apareciendo y que afecten a los principales sistemas operativos y software comercial: dicha información se deberá proporcionar a través de un servicio de alerta temprana que publique vulnerabilidades antes de que sean reconocidas por los fabricantes de software.
- Reputación web: mediante calificación de la reputación de los dominios web, URLs y páginas dentro de una URL para reflejar la posibilidad de que sea un sitio de *phishing*, esté infectado por malware o presente cualquier otra forma de mala intención
- Reputación de red: mediante identificación de aquellas conexiones que constituyan una amenaza, como en el caso de una conexión asociada al control de redes (botnet) o patrones conocidos de ataques de denegación de servicios.

La base de datos de inteligencia de seguridad del fabricante estará distribuida en múltiples ubicaciones para asegurar la alta disponibilidad en el acceso a través de Internet. Complementariamente se deberá permitir disponer de una réplica de dicha base de datos en la plataforma del Ayuntamiento, que se actualizará de manera automática. Serán actualizaciones incrementales, con una frecuencia mínima diaria, pudiendo realizarse con mayor frecuencia si es necesario (p.ej. en el caso de una prevención temprana o por resolución de una incidencia ante un ataque de virus).

3.2 REQUISITOS TÉCNICOS.

El antivirus corporativo ofertado deberá incluir los siguientes componentes de software para la protección específica de cada uno de los entornos, considerando los siguientes requisitos:

3.2.1 Protección de equipos con sistema operativo MS WINDOWS.

Se requerirá una solución de protección para puestos de trabajo PC y portátiles (Windows XP, 7 y 8), así como servidores (Windows 2003 y 2008 Server), en modalidades de 32/64 bits, ante todo tipo de virus, spyware, rootkits y cualquier tipo de malware.

Dicho software deberá ir integrado en un único agente instalado en el equipo, con las siguientes características y funcionalidades:

- Exploración antivirus para la detección, limpieza y eliminación de todo tipo de virus, troyanos, gusanos y herramientas de acceso remoto que puedan dañar los equipos a través de ejecución de aplicaciones, navegación, clientes de correo (Outlook) y dispositivos extraíbles.
- Estará basado tanto en patrones de firmas como en tecnología heurística con capacidad de detección de virus en archivos comprimidos, exigiéndose compatibilidad con múltiples formatos de compresión (al menos ZIP, RAR, LHZ, ARJ, ACE, TAR, GZIP) y posibilidad de dejar los archivos infectados en una carpeta local de cuarentena.
- Servicio de reputación de archivos o protección inteligente: El motor antivirus empleará la reputación de archivos para determinar las medidas a tomar (como eliminar, limpiar o poner en cuarentena) en función de la directiva local.
- Antispyware dedicado a la detección y limpieza de todo tipo de spyware en tiempo real.
- Componente para la detección y limpieza de rootkits.
- Como componente opcional: cortafuegos integrado, que permitirá la selección mediante reglas configurables del tráfico de red, que se permite o deniega en entrada/salida del equipo. Las reglas de cortafuegos permitirán bloquear tráfico para evitar la explotación de vulnerabilidades encontradas en el equipo, tanto a nivel de sistema operativo como de aplicaciones instaladas.
- Sistema de detección y prevención de intrusiones a nivel de equipo (IDS/IPS). Se podrán realizar:
  - Escaneos de los parches de seguridad del sistema operativo y máquina virtual JAVA, aplicados en el equipo para comprobar si el sistema está actualizado o desprotegido ante nuevas vulnerabilidades aparecidas.
  - Funciones de parcheado virtual, mediante la posibilidad de aplicar reglas que mitiguen las vulnerabilidades aparecidas, antes de aplicar la correspondiente actualización de seguridad del sistema operativo y/o de la máquina virtual JAVA.
- Monitorización del comportamiento, de forma que se pueda denegar mediante reglas que ciertas partes críticas del sistema (memoria, ficheros de sistema y ejecutables) puedan ser modificadas indebidamente.
- Control de aplicaciones: capacidad para definir listas blancas y listas negras de aplicaciones, con el objeto de bloquear su posible ejecución en cualquier equipo o grupo de equipos.
- Análisis de todos los archivos en tiempo real. Se deberá permitir la ejecución de análisis planificados o bajo demanda del usuario. El análisis incluirá todos los archivos abiertos o en ejecución. Se permitirá excluir del análisis las carpetas, rutas o archivos que se indiquen.
- Análisis en tiempo real durante la navegación web del código Active X y JavaScript asociados a las páginas accedidas.
- Actualización automática del agente a partir de la base de datos de inteligencia de seguridad:
  - Actualización con frecuencia, al menos diaria, de una base de datos local de patrones de virus y de spyware.
  - Revisión/actualización periódica de parches y nuevas versiones de los motores.
- Las actualizaciones deberán ser automáticas, desatendidas y con posibilidad de emplear diferentes orígenes de la base de datos de inteligencia de seguridad. En el caso de equipos conectados a la red corporativa municipal, la actualización se realizará preferentemente a través de los servidores internos y para ordenadores portátiles, cuando no estén conectados a la red corporativa, a través de Internet.
- El agente instalado en cada equipo dispondrá de un interfaz en idioma español que permita al usuario final realizar algunas tareas básicas, como la verificación y actualización de la versión de los componentes o lanzar un análisis antivirus.
- El agente antivirus deberá instalarse y desinstalarse con facilidad, mediante un mecanismo de instalación y despliegue automático, con opción manual para casos puntuales. Este mismo mecanismo o herramienta de instalación/desinstalación se empleará al término del presente contrato, para la desinstalación completa del agente en todos los equipos corporativos instalados.

3.2.2 Protección de entornos virtualizados.

Dentro de los requisitos, se incluyen las capacidades de *'Exploración antivirus'* descritas en el apartado de 3.2.1. *"Protección de equipos con sistema operativo MS Windows".*

Se ofrecerán soluciones optimizadas de antimalware para los entornos virtuales utilizados en el Ayuntamiento:

- Virtualización de servidores: VMware vSphere v.3.5 y 5.
- Virtualización de escritorio - VDI (con sistema operativo Windows): Si bien no se requiere inicialmente el suministro de licencias para este entorno, la solución propuesta por el licitador debe soportarlo, ya que las licencias podrán ser solicitadas por el Ayuntamiento durante el periodo de vigencia del presente contrato. En este sentido, deberá especificarse con qué software de virtualización (VDI) está certificado el funcionamiento de la solución antivirus.

En ambos entornos, la solución antimalware deberá cumplir las siguientes funcionalidades optimizadas para virtualización:

- Escaneos aleatorios o alternados en las máquinas virtuales alojadas en un host físico, para evitar el colapso de recursos.
- Actualización inteligente del archivo de firmas y del motor, de forma que se permita una de estas opciones:
  - Actualización en una de las máquinas, que luego se encargue de distribuirla al resto de máquinas virtuales.
  - Actualización aleatoria o distribuida, para no coincidir y evitar un colapso de red.

Además, para el entorno VMware vSphere v.3.5 y 5, la solución antimalware permitirá la instalación de agentes ligeros que consuman los mínimos recursos de la máquina virtual. Para ello, la protección antimalware se deberá delegar en otra máquina virtual de seguridad en formato de dispositivo virtual (*virtual appliance*), que supervise y realice los análisis antivirus de las máquinas virtuales alojadas en el mismo host ESX. Se permitirá una de estas alternativas:

- Arquitectura híbrida, compuesta por una máquina virtual de seguridad, con software antivirus y agentes ligeros del propio fabricante en cada máquina virtual.

- Integración con el producto VMware vShield Endpoint, que aporta un agente ligero propio de vShield Endpoint. Se creará una *appliance* virtual de seguridad por cada host ESX, con software antivirus del fabricante, que se encargue de la protección antimalware de todas las máquinas virtuales desplegadas en él, mejorando el consumo de recursos y rendimiento. Esta solución deberá permitir no tener que instalar agente del fabricante antivirus en las máquinas virtuales, únicamente el agente ligero de vShield Endpoint. El Ayuntamiento valorará positivamente la propuesta de esta opción frente a la de arquitectura híbrida.

Para el entorno de escritorios virtualizados VDI, se requerirá la capacidad de creación de una lista blanca de ficheros, a partir de una plantilla imagen de máquina virtual, evitando escaneos duplicados.

3.2.3 Consola de gestión del antivirus corporativo.

Tal como se ha indicado anteriormente, la solución propuesta se administrará de forma centralizada, utilizando la consola de gestión del antivirus corporativo, que se instalará sobre una plataforma de sistema operativo Windows, constituyendo el punto central de gestión y control de actualización de todos los productos.

Será necesario incluir las funcionalidades siguientes:

- Asistente de instalación, actualización de versiones de todos los productos, tanto para la propia consola como para desplegar automáticamente agentes de protección antimalware en los equipos conectados a la red corporativa, al menos para los agentes en equipos Windows y servidores Windows virtuales.
- Gestor de descargas: la propia consola administrará el software de la solución, descargando actualizaciones automáticamente para todos los productos gestionados y de la propia consola.
- Distribución automática y planificada a los equipos gestionados de información de la base de datos de inteligencia de seguridad (patrones de firmas).
- Descubrimiento y gestión del inventario hardware y software de los equipos que utilizan la solución.
- Despliegue y control de software de terceros en los equipos corporativos, como p.ej: maquina virtual JAVA, productos Adobe, etc.
- Posibilidad de lanzar en tiempo real tareas de limpieza y reparación en los equipos.
- Gestión de epidemias: capacidad de configuración de las políticas de prevención de epidemias (bloqueo de acceso a archivos y puertos, principalmente), permitiendo activar el servicio al administrador cuando aparezca una alerta de epidemia.
- Información accesible en tiempo real, por medio de paneles de información y cuadros de mando, sobre el estado actual del parque de equipos gestionados e infecciones producidas y remediadas.
- Recepción centralizada de información de actividad (*logs*) para todo el parque informático. Integración con herramientas de gestión de eventos y análisis de dicha información.
- Generación de informes:
  - Personalizados mediante consultas directas a la base de datos de equipos gestionados, por medio de plantillas.
  - Informes programados sobre los resultados del análisis.
  - Informes en tiempo real sobre el estado de actualización del parque.
  - Formatos: al menos PDF, MS Excel, CSV y HTML.
- Acceso a la consola de gestión vía web https (gestión segura SSL).
- Posibilidad de organizar las tareas de administración y establecimiento de políticas de seguridad en base a agrupaciones definidas por direccionamiento IP y perfiles de directorio activo.
- Gestión centralizada de las licencias del producto de protección para puestos de trabajo.

4 REQUISITOS DE IMPLANTACIÓN Y PUESTA EN SERVICIO.

4.1 SUMINISTRO.

- Suministro del software ofertado con su correspondiente documentación y licencias, manuales de instalación, despliegue y actualización, etc.
- El suministro se dará por entregado e instalado tras la supervisión y correspondiente informe del Servicio de Nuevas Tecnologías y Procesos.

4.2 PLAN DE IMPLANTACIÓN.

Las empresas licitadoras presentarán un Plan de Implantación detallado, describiendo las actividades y tareas a realizar, garantizando los siguientes puntos:

- Desinstalación de la actual solución de antivirus de todos los equipos y servidores.
- Suministro, instalación y configuración de todos los elementos detallados en el presente pliego.
- Plan de migración a la nueva solución.
- Mínimo impacto en el servicio.

4.3 PLAN DE CALIDAD Y PRUEBAS.

El licitador deberá presentar en su oferta un Plan de Pruebas que especificará tanto las pruebas unitarias iniciales, necesarias para poder detectar de manera anticipada cualquier error o mal funcionamiento del equipamiento propuesto para este proyecto, así como las pruebas funcionales y de integración necesarias para asegurar el cumplimiento de los requerimientos detallados en el presente pliego.

El propósito del Plan de Pruebas definido es asegurar que el equipamiento ha sido correctamente configurado y que, en conjunto, la solución opera de la manera esperada, permitiendo su paso a producción con los servicios definidos en el marco de este proyecto.

Para garantizar la calidad en la ejecución del proyecto, el adjudicatario se responsabilizará de que su personal especializado lleve a cabo las tareas siguientes:

- Planificación de las actividades de calidad.
- Control de calidad durante todas las etapas y fases del proyecto.
- Revisión de entregables y control de hitos.
- Revisión y control de calidad previos a la entrega del documento final y cierre de proyecto.

Durante la ejecución de los trabajos, el Ayuntamiento podrá establecer las acciones de garantía de calidad que estime oportunas sobre la actividad desarrollada y los productos obtenidos. A tal fin, podrá dedicar a la realización del proyecto los recursos económicos, materiales y personales que considere convenientes para garantizar su correcta ejecución.

Al objeto de justificar la conformidad del licitador con determinadas normas de garantía de calidad, se valorará la aportación de certificados de garantía de calidad, basados en la serie de normas Internacionales ISO 9000, europeas EN 29000 o españolas UNE 66900 y expedidos por organismos conformes con la serie de normas europeas EN 45000. No obstante, se podrán tener en cuenta certificados de calidad equivalentes, expedidos por otros organismos de normalización establecidos en cualquier Estado Miembro de la Unión Europea.

Adicionalmente, el licitador deberá aportar los certificados que le hayan sido otorgados por parte del fabricante de la solución.

4.4 PLAN DE FORMACIÓN.

Se establecerá, de común acuerdo entre el Ayuntamiento y la empresa adjudicataria, un Plan de Formación sobre la solución implantada, que será aprobado por el Ayuntamiento.

La empresa adjudicataria impartirá dicha formación en las dependencias municipales a los administradores y personal del servicio técnico de mantenimiento informático.

En el Plan de Formación deberán estar contemplados los aspectos más importantes de la tecnología antivirus implantada, tales como:

- Despliegue e instalación de los productos contratados.
- Administración de la solución software.
- Manejo de la consola de gestión centralizada.

El período de formación no deberá ser inferior a dos jornadas laborales.

4.5 GARANTÍA Y MANTENIMIENTO.

Las empresas licitadoras presentarán un Plan de Garantía y Mantenimiento de la solución propuesta, que asegure su óptimo y continuo funcionamiento e incluya una respuesta inmediata ante los posibles problemas que pudieran producirse. Por tanto, durante el periodo de garantía de la solución, se prestará el servicio de mantenimiento de la misma, que incluirá sin coste adicional para el Ayuntamiento una serie de servicios tales como:

- Garantía de todos los bienes suministrados.
- Mantenimiento correctivo y evolutivo de la solución. Soporte en la planificación de migración de versiones, instalación de productos y parches y consultas de configuración. Actualización de todos los componentes y bases de datos de la solución antivirus.
- Acceso directo por parte del Ayuntamiento a la base de conocimientos oficial del fabricante.
- Servicio de alertas sobre las últimas vulnerabilidades/amenazas potenciales detectadas por el fabricante, con el fin de actuar de forma preventiva y correctiva.
- **Soporte técnico** de la solución, en idioma castellano, para resolución de cualquier incidencia/consulta relacionadas con la instalación y correcto funcionamiento de los productos instalados. Más concretamente:
    - Atención de incidencias, como p.ej. las ocasionadas por mal funcionamiento de algún componente de la solución, malware no detectado y control de epidemias puntuales.
        - Asistencia remota para limpieza y reparación: posibilidad de acceder, con el permiso del usuario, al equipo infectado para limpiarlo de todo virus y código malicioso que no se haya podido limpiar en tiempo real mediante el motor antivirus. Se deberán reparar los daños del sistema, finalizar todos los procesos víricos y subprocesos de memoria, reparar el registro, eliminar los servicios y archivos introducidos por el virus y restaurar los archivos dañados.
        - Se requerirá el establecimiento de un procedimiento de recogida de indicios en equipos sospechosos, posiblemente infectados, para que sean analizados por el

laboratorio del fabricante a fin de ofrecer un remedio desarrollando un parche en caso de encontrar código malware.

- Resolución de consultas técnicas especializadas para la configuración y uso de los productos.
- Asistencia para el despliegue de la solución en el nuevo hardware y entorno de virtualización de servidores previsto durante la ejecución del contrato.
- Canales de acceso al servicio: web, correo electrónico y atención telefónica.
- Horario del servicio: 8x5 (de 8:00 a 15:00 horas, de lunes a viernes).
- El Ayuntamiento asignará un nivel de prioridad/severidad para cada caso abierto, que determinará los tiempos máximos de respuesta y de resolución (ambos tiempos contabilizarán desde el momento de apertura del incidente a través de los canales establecidos):

Tipo evento	Tiempo de respuesta	Tiempo de resolución
Consulta/petición de información	12 horas	48 horas
Incidencia leve	2 horas	24 horas
Incidencia media	1 hora	8 horas
Incidencia grave	1 hora	4 horas

El Ayuntamiento podrá requerir el cumplimiento de los tiempos de resolución establecidos en aquellos casos en que la incidencia sea causada por la infección de un virus conocido, debiendo aplicar los mecanismos de limpieza y reparación que tenga para el mismo, o por fallo de alguno de los productos instalados, en los que las soluciones aplicables estén basadas en el empleo de código oficialmente liberado por el fabricante y estén recogidas en su base de datos de conocimiento oficial.

En otros casos, como en el caso de aparición de un nuevo virus, se requerirá el compromiso de realizar el escalado interno de la incidencia para su análisis y desarrollo de solución. Simultáneamente el contratista deberá proponer alternativas que permitan la resolución temporal del problema, a fin de poder mantener los niveles de servicio; en todo caso, su implantación deberá contar con la aprobación del gestor técnico designado por el Ayuntamiento.

- Asistencia presencial, por parte de personal certificado en la solución, en alguno de estos supuestos:
  - Despliegue inicial e instalación de todos los productos.
  - Cuando una incidencia puntual no haya sido resuelta satisfactoriamente mediante el procedimiento propuesto a los técnicos municipales, ni por acceso remoto al equipo afectado.

5 ANEXO I: PARQUE INFORMÁTICO MUNICIPAL.

Para conformar la oferta económica, el licitador incluirá todos los ítems descritos a continuación (parque informático actual), teniendo en cuenta las siguientes consideraciones:

- El inventario podrá sufrir un incremento del 2% durante el periodo de ejecución del contrato, y este incremento estará incluido en el importe de licitación, no suponiendo un coste adicional para el Ayuntamiento. El aumento porcentual previsto marcará un valor económico de referencia (máximo) del que podrá disponer el Ayuntamiento según el incremento real de su parque. P.ej: El 2% de aumento no producido en servidores podrá destinarse a aumentar por encima del 2% el número de licencias para puestos de trabajo.
- Las licencias serán intercambiables y se adecuarán a la evolución (migración) de los sistemas operativos y software de virtualización de los equipos durante la duración del contrato, sin coste adicional para el Ayuntamiento.
- Se facturarán únicamente las licencias reales suministradas, aplicando los prorrateos correspondientes.

5.1 SERVIDORES Y PUESTOS DE TRABAJO.

La siguiente tabla incluye la relación de servidores y puestos de trabajo (volumen y sistema operativo):

Sistema Operativo	Número de equipos
SERVIDORES:	
Windows 2003 Server SP3 Físicos (se migrarán a Windows 2008)	7
Windows 2003 Server SP3 Virtuales VMware (se migrarán a Windows 2008)	18
PUESTOS DE TRABAJO:	
Windows XP (se migrarán a Windows 7)	550
Windows 7	150
MAC	2
Terminales VDI (Windows 7)	50 (*)

(*) Terminales VDI: Tal y como se ha indicado anteriormente, no deben suministrarse estas licencias hasta el momento que el Ayuntamiento las demande.

5.2 PLATAFORMA DE VIRTUALIZACIÓN VMWARE.

El Ayuntamiento cuenta actualmente con cuatro servidores HP como ESX para la plataforma de virtualización VMware con vCenter v.3.5, con las siguientes características:

- 1 servidor HP Proliant DL385 G1: AMD Opteron 280 Quad Core 2,4GHz, 12 GB de RAM.
- 2 servidores HP DL380 G5: Intel Xeon Quad Core E5345 2,33GHz, 16GB de RAM.
- 1 Servidor HP DL385 con 8GB de RAM.

Está prevista la migración de VMware a la versión 5, junto con la adquisición de nuevo hardware de servidores para soportarla.