MUNICIPALIDAD DISTRITAL DE MIRAFLORES

MIRAFLORES
CIUDAD HEROICA

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE

NÚMERO: P002-2011-GSTI

"ADQUISICION DE LICENCIAS DE SOFTWARE ANTI-VIRUS, ANTI-SPAM Y CONTROL DE ACCESO A RED"

MUNICIPALIDAD DE MIRAFLORES
JAVIER CONSTANTINO CARRANZA VERAMENDI
Gerente
V°B°
Gerencia de Sistemas y Tecnología de la Información

Tabla de Contenido

Página

MUNICIPALIDAD DE MIRAFLORES
JAVIER CONSTANTINO CARRANZA VERAMENDI
Gerente
V°B°
Gerencia de Sistemas y Tecnologías de la Información

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE LICENCIAS DE SOFTWARE ANTI-VIRUS, ANTI-SPAM Y CONTROL DE ACCESO A LA RED

1. Nombre del área

El área encargada de la evaluación técnica para la adquisición de LICENCIAS DE SOFTWARE ANTI-VIRUS, ANTI-SPAM Y CONTROL DE ACCESO A LA RED es la Gerencia de Sistemas y Tecnologías de la información.

2. Nombre y cargo de los responsables de la evaluación.

El responsable de la evaluación es el Sr. Javier Vílchez López cuyo cargo es Coordinador de Soporte y Redes

3. Fecha

La fecha del presente informe es 08 de Noviembre de 2011.

4. Justificación

En la actualidad contamos con 550 equipos las cuales forman parte de la red informática de la municipalidad de Miraflores (computadoras de escritorio, portátiles y servidores) las cuales se debe proteger y garantizar su buen funcionamiento y operatividad para el buen desarrollo de las operaciones propias de la entidad.

Hecho el análisis de la situación de la seguridad actual y teniendo como horizonte la protección a nuevos tipos de amenazas tanto de malware como a la protección de la información; se requiere contar a nivel de las estaciones de trabajo y servidores con una solución que permita implementar un entorno optimizado y que de bajo impacto en los recursos de los equipos que proteja frente a virus, spyware, rootkits, gusanos, protección en la navegación y cualquier otro tipo de contenido maliciosos que dañen o afecten la integridad de la información, así como también se pueda controlar el uso y/o la instalación de aplicaciones que causan un impacto negativo en la productividad de los usuarios y en el uso del ancho de banda de la red.

La solución debe asegurar la seguridad identificando las amenazas o debilidades de la infraestructura de red y deberá ayudar inmediatamente a tomar acciones previniendo incidentes antes que las amenazas informáticas impacten negativamente en los recursos (activos) de la red.

De la misma forma se requiere que la solución permita la implementación del Control de Acceso a la Red, también conocido como NAC en todas la áreas de la institución para lo cual deberá incorporar un agente NAC que funcione con los principales equipos de comunicación de red

MUNICIPALIDAD DE MIRAFLORES
JAVIER CONSTANTINO CARRANZA VERAMENDI
Gerente
V°B°
Gerencia de Sistemas y Tecnologías de la Información

incluyendo CISCO, 3COM, Alcatel, D-Link, etc. sin requerir el cambio de dichos equipos bajo ningún concepto.

También se ha podido ver que se requiere contar con una mejor protección a nivel perimetral con una solución que incluya appliances y software para la protección contra spam, malware, spyware y ataques de denegación de servicio que funcionen en modo redundante y en cluster en forma automatizada con el fin de asegurar la disponibilidad de las comunicaciones en la empresa.

Finalmente, con el objetivo de asegurar la integridad, disponibilidad y confidencialidad de la información importante, así como el normal desarrollo de sus funciones, ser requiere contar con una solución de seguridad anti-virus, anti-spam y de control de acceso a la red corporativa. (Dominio 10 Gestión de Comunicaciones y Operaciones. Objetivo de Control 10.4 Protección contra software malicioso de la Norma Técnica Peruana NTP-ISO/IEC 17799-2007 EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información).

5. Alternativas

Para la selección de alternativas, se tomó como base a los fabricantes de soluciones líderes, según el Cuadrante Mágico de Gartner que tuvieran por lo menos un representante autorizado en el Perú.

Las alternativas seleccionadas se muestran a continuación:

Fabricante	Producto
Kaspersky	Kaspersky OpenSpace
Sophos	Sophos Endpoint + Email Security and Control
Panda	Panda Cloud Protection

6. Proceso de evaluación de software

El proceso de evaluación de software se desarrolló sobre la base de la Guía de Evaluación de Software para la Administración Pública (RM N° 139-2004-PCM).

6.1. Propósito de la evaluación

El propósito de la evaluación es identificar las funcionalidades mínimas que debe cumplir la Solución de Software Anti-Virus, Anti-Spam y Control de Acceso a la Red.

6.2. Tipo de producto

SOLUCIÓN DE SOFTWARE ANTI-VIRUS, ANTI-SPAM Y CONTROL DE ACCESO A LA RED

MUNICIPALIDAD DE MIRAFLORES
JAVIER CONSTANTINO CARRANZA VERAMENDI
Gerente
V°B°
Gerencia de Sistemas y Tecnologías de la Información

6.3. Especificación del modelo de calidad y selección de métricas

Se ha definido la siguiente relación de atributos que deberá cumplir la SOLUCIÓN DE SOFTWARE ANTI-VIRUS, ANTI-SPAM Y CONTROL DE ACCESO A LA RED

Modelo de Calidad (de acuerdo a la RM N° 139-2004-PCM)		
Item	**Atributo**	**Características Técnicas**
ATRIBUTOS INTERNOS		
1	Sistemas operativos de estaciones de trabajo	▪ Microsoft Windows 2000 Professional. ▪ Microsoft Windows XP Professional. ▪ Microsoft Windows Vista y Microsoft Windows 7. En versiones de 32 y 64 bits.
2	Sistemas operativos de servidores de Red	▪ Microsoft Windows 2000 Server ▪ Microsoft Windows 2003 Server ▪ Microsoft Windows 2008 Server ▪ Red Hat Enterprise 4/5 ▪ Suse Enteprise Linux 9/10 En versiones de 32 y 64 bits.
3	Protección y defensa frente a malware en portátiles, computadoras de escritorio y servidores.	▪ La solución de seguridad para estaciones y servidores es de tipo integrada; es decir incluye un único agente que brinda protección frente a virus, spyware, adware, rootkits, comportamientos sospechosos, filtrado de seguridad URL, detección Web de ataques de scripts maliciosos y aplicaciones potencialmente peligrosas en todos los protocolos de la red. ▪ La solución cuenta con una cuarentena de usuario final que permita controlar y/o autorizar el uso de ciertas aplicaciones no deseadas. ▪ La solución tiene versiones para Linux el cual cuenta con un módulo de escaneo de archivos de alto rendimiento, estabilidad y eficacia el cual debe permitir el escaneado en acceso, en demanda y programado de unidades locales, extraíbles y compartidas (como NFS y Samba), y otros sistemas de archivos. La versión para Linux debe poder ser configurada y administrada desde la consola central. ▪ La solución puede actualizarse desde una consola central y desde la web del fabricante simultáneamente con el fin de asegurar una completa protección aún cuando la consola central no se encuentre activa. ▪ La solución de seguridad instalada en todas las plataformas requeridas debe notificar los eventos de virus, spyware, adware, aplicaciones no deseadas, intrusiones, cambios en la configuración del cliente de seguridad a la consola central. ▪ La solución está incluido en el Cuadrante Mágico de Gartner de Plataformas de Protección de Punto Final como Líder en los últimos 2 reportes publicados por dicha compañía (2009 y 2010).

MUNICIPALIDAD DE MIRAFLORES
JAVIER CONSTANTINO CARRANZA PERAMENDI
Gerente
V°B°
Gerencia de Sistemas y Tecnologías de la Información

		▪ El sistema de filtrado URL y el de detección Web de Ataques de Script maliciosos debe denegar el acceso al sitio y deberá mostrar una página HTML de bloqueo en el navegador de internet (IE, Mozilla, Chrome, Opera, etc) donde le indique al usuario la razón por la que no ha podido acceder a dicha página. *El postor deberá incluir la captura de la pantalla del funcionamiento de esta característica.* ▪ La solución deberá incorporar un sistema para el Control de la navegación web el cual deberá estar integrada a la consola de la solución. Además esta solución deberá contar con al menos 12 categorías predefinidas de sitios web las que deben ser mantenidas por el fabricante y son: 1. Sitios web de adultos o sexo 2. Sitios web de Hacking 3. Sitios web de Phishing 4. Sitios web de juegos 5. Sitios web de proxys anónimos 6. Sitios web de Drogas 7. Sitios web de spam 8. Sitios web de Actividades Criminales 9. Sitios web con material Ofensivos 10. Sitios web de Violencia 11. Sitios web de intelerancia o raciales 12. Sitios web de Alcohol y tabaco ▪ La solución cuenta con la Certificación Checkmark Checkmark 100% por la detección de programas espía. *El postor deberá presentar una impresión de la página web del certificador donde aparezca registrado.* ▪ La solución permite la creación de CD, DVD o USB Booteables de emergencia mediante imágenes .ISO u otro formato de grabación de medios para la recuperación y limpieza de equipos infectados. La creación de dichas imágenes no deberá depender de productos de terceros ni requerir licencias de productos adicionales al del propio fabricante.
4	Firewall	▪ La solución incluye un Firewall Personal del mismo fabricante. ▪ El firewall personal es administrado centralizadamente desde la consola de gestión. ▪ El firewall permite bloquear, autorizar aplicaciones y puertos específicos tanto local como centralizadamente. ▪ El firewall permite trabajar en modo oculto. ▪ El firewall permite ser configurado en modo control o auditoría con la finalidad de recoger información de aplicaciones, puertos y protocolos usados en los equipos de la red y que permite crear políticas de seguridad en forma rápida y simple. ▪ El firewall automáticamente se reconfigurarse con otro tipo de política de protección de acuerdo a la ubicación donde se encuentre. Esta reconfiguración deberá realizarse

MUNICIPALIDAD DE MIRAFLORES
JAVIER CONSTANTINO CARRANZA VERAMENDI
Gerente
V°B°
Gerencia de Sistemas y Tecnologías de la Información

		mediante la detección de la MAC address del Gateway de red o del DNS.
5	Sistema de prevención de intrusos de hosts – HIPS y detección de desbordamiento de buffers (BOPS – Buffer Overflow Protection System)	▪ La solución incluye una tecnología de detección de intrusos de host (HIPS) incorporado en el agente anti-malware que brinde protección en acceso. ▪ La solución deberá incluir una tecnología para la detección de intentos de desbordamiento de buffers (BOPS – Buffer Overflow Protection System) incorporado en el agente anti-malware. ▪ La solución cuenta con una tecnología de prevención y detección de intrusos que detecta malware "antes de su ejecución (pre-execution)" y "en ejecución (on-execution)". ▪ El sistema HIPS está integrado en el agente antimalware y permite configurarse en modo bloqueo de procesos o en modo solo alerta. ▪ *El sistema HIPS no requiere ejecutar o instalar agentes o programas adicionales al motor antimalware ni ejecutarse en forma programada para la prevención y/o detección de intrusos de hosts. Tampoco deberá requerir la instalación de un cliente firewall para que esta funcionalidad se active.*
6	Control de dispositivos	▪ Para la protección contra el malware en dispositivos externos la solución incluye un sistema de control de dispositivos que detecta el uso de dispositivos USB, Grabadores de CD/DVD, Floppy Disk, Lectores de CD/DVD, HDD Externos y dispositivos Wireless. ▪ El sistema de control de dispositivos cuenta con opciones para Permitir, Bloquear, Alertar y Configurar en modo Solo-Lectura los dispositivos indicados. ▪ El sistema de control de dispositivos permite la autorización de dispositivos específicos (basados modelo específico o marca) la utilización de dispositivos cifrados e incluso controlar el uso de interfaces de red como los módems convencionales y los módems 3G. ▪ El sistema de control de dispositivos está integrado en el agente antimalware, es decir, no requiere la instalación de programas adicionales en los equipos. ▪ El sistema de control de dispositivos cuenta con opciones para evitar el modo "puente-de-red" para dispositivos de red Wireless y Modems, incluyendo los 3G, que permita evitar que los usuarios incumplan las políticas corporativas de acceso a internet.
7	Protección contra ataques de día cero.	▪ La solución cuenta con tecnologías de detección proactiva de amenazas conocidas y basadas en la nube (in-the-cloud) del mismo fabricante. ▪ La solución ofrece una rápida y eficaz detección de archivos sospechosos mediante la comprobación instantánea de archivos sospechosos en la nube.

MUNICIPALIDAD DE MIRAFLORES
JAVIER CONSTANTINO CARRANZA ZERAMENDI
Gerente
V°B°
Gerencia de Sistemas y Tecnología de la Información

		▪ El sistema de protección de filtrado URL realiza comprobaciones de direcciones web sospechosos (hackeadas, que albergan malware, etc.) en forma automática hacia la nube (base de datos del fabricante) para una rápida y efectiva protección contra este tipo de amenazas.
8	Seguridad	▪ La solución es capaz de evitar que sus procesos, servicios, archivos, o archivos de registro puedan ser detenidos, deshabilitados, eliminados o modificados, para de esta manera garantizar su funcionamiento ante cualquier tipo de ataque de virus. ▪ La solución cuenta contar con medidas de seguridad para que el usuario de la estación de trabajo, sea este el administrador de la red o la PC no deje sin efecto políticas de seguridad corporativas. ▪ La desinstalación del módulo cliente y sus componentes debe estar protegido con una clave de seguridad asignada por el administrador de la solución. Esta clave puede ser configurada para un grupo específico o todos los equipos en la red. ▪ La seguridad de la solución se integra el Directorio Activo de la red y con el sistema de grupos de Microsoft para una mejor y efectiva protección. ▪ El usuario no puede realizar una configuración particular de la solución a menos que el administrador de la red le otorgue privilegios ya sea localmente o mediante la integración con el Directorio Activo de Microsoft. ▪ La solución cuenta con un sistema de administración de parches de múltiples fabricantes como Microsoft, Adobe, Mozilla, Apple y Citrix que permita conocer la lista de parches que no se han aplicado en los equipos administrados. ▪ La solución de administración de parches deberá mostrar además la lista de vulnerabilidades que son aprovechadas por atacantes o malware específicos. *El postor deberá adjuntar una captura de pantalla donde se muestre el funcionamiento de esta característica. No se aceptarán propuestas que no incluyan dicha captura.* ▪ Cualquier intento de vulneración de las características de seguridad deberá ser reportado a la Consola de Gestión Centralizada. *El postor deberá incluir una captura de pantalla del funcionamiento de esta característica.*
9	Control de aplicaciones	▪ La solución cuenta con un sistema que permite controlar el uso de determinados tipos de aplicaciones en los equipos de la red. ▪ El sistema de control de aplicaciones permite controlar y bloquear el uso de aplicaciones que causan un impacto negativo en el trabajo de los usuarios, en el uso del ancho de banda en la red y el incumplimiento de políticas corporativas las cuales se encuentran agrupadas o

MUNICIPALIDAD DE MIRAFLORES
JAVIER CONSTANTINO CARRANZA VERAMENDI
Gerente
V°B°
Gerencia de Sistemas y Tecnologías de la Información

		categorizadas por tipo de programas; al menos como Programas P2P, Mensajería, Proxy's y Maquinas Virtuales. ▪ La solución permite limpiar y desinstalar remotamente las principales aplicaciones P2P controladas (Peer-to-peer) desde la Consola de Administración. ▪ La agrupación o categorización de tipos de aplicaciones es mantenida por el fabricante y se actualizan en forma automática. ▪ La entidad puede solicitar al fabricante la inclusión de nuevos programas y/o aplicaciones que considere que deben bloquearse y que se requiera incluir en dicho sistema.
10	Control de acceso a la red	▪ La solución cuenta con la capacidad de integración con las políticas de seguridad de Cisco NAC. ▪ La solución incorpora un Agente de Control de Acceso a la Red del mismo fabricante. Este agente también conocido como "Agente NAC" puede mantener todos los equipos sean estos administrados, no administrados o invitados (equipos que se conectan a la red esporádicamente) en buen estado y con la protección antivirus actualizada, así mismo, deberá asegurar que se corrijan las vulnerabilidades encontradas. ▪ El Agente de Control de Acceso a la Red permite establecer políticas para verificar al menos: » Si el antivirus esta activo y actualizado. » Si el equipo cliente tiene activado el sistema de actualización de parches del sistema operativo. » Si el cliente firewall está activo. » Si el equipo tiene activado algún sistema de encriptación de información. ▪ La solución NAC permite integrarse con el sistema DHCP de Microsoft para establecer políticas de control de acceso a la red. ▪ La solución NAC es multi-fabricante, es decir, no depende de ningún hardware adicional, ni modelo de dispositivo de red (concentrador, switch, etc.) para su funcionamiento.
11	Control de fuga de información(DLP)	▪ La solución incluye un sistema del para el control de fuga de datos conocido como DLP. ▪ El Sistema de Control de Fuga de Datos permite controlar, restringir y auditar la información que es copiada o enviada fuera de la red corporativa mediante el uso de dispositivos externos como USB, Internet, Correo Electrónico y Mensajería Instantánea. ▪ El Sistema de Control de Fuga de Datos es del mismo fabricante y deberá poder controlar la información saliente por tipo de contenido y tipo de archivo. ▪ El sistema de control de fuga de datos incluye listas de control preconfiguradas para la elaboración rápida de

MUNICIPALIDAD DE MIRAFLORES
JAVIER CONSTANTINO CARRANZA ERAMENDI
Gerente
V°B°
Gerencia de Sistemas y Tecnologías de la Información

		políticas corporativas. ▪ El sistema de control de fuga de datos está incorporado en el agente antimalware, es decir, no se requiere la instalación de ningún agente adicional en los equipos. ▪ La administración de este sistema se realiza desde la Consola de Administración Central de la solución de seguridad antimalware.
ATRIBUTOS EXTERNOS		
12	Instalación y despliegue del software	▪ La instalación del software a las computadoras de los usuarios se puede realizar mediante: » Instalación automática mediante la sincronización con el Directorio Activo de Microsoft. » Instalación remota desde la Consola de Administración. » Instalación manual mediante CD o recurso UNC. ▪ El instalador incorpora un sistema de *Eliminación de Software de Seguridad de Terceros* (agentes antimalware y firewall) que permita desinstalar automáticamente otros productos de seguridad sin requerir realizar manualmente dicho proceso con el fin de optimizar el proceso de despliegue de la solución. ▪ La solución permite crear a pedido de la institución instaladores que permitan el despliegue del producto mediante CD o vía Web. Estos instaladores pueden ser personalizados y permiten por ejemplo contener información relativa a la propiedad de la institución. ▪ El sistema de *Eliminación de Software de Seguridad de Terceros* es del mismo fabricante. ▪ El sistema de *Eliminación de Software de Seguridad de Terceros* está incorporado en el sistema de instalación del agente antimalware, es decir, puede activarse o desactivarse al momento del despliegue de la solución. ▪ El sistema de *Eliminación de Software de Seguridad de Terceros* no requiere la implementación, configuración o instalación por separado de consolas, programas o agentes para este fin. ▪ El instalador permite la instalación del Agente de Control de Acceso a la Red durante el despliegue de la solución.
13	Actualización de firmas y nuevas versiones del producto.	▪ Las actualizaciones se realizan automáticamente (programadas) y manualmente del fichero de firmas de virus y del motor de escaneado de malware en los servidores y estaciones de trabajo desde Internet. ▪ La actualización de firmas automáticas deberá realizarse cada 30 minutos o menos. ▪ El tamaño de las actualizaciones de firmas de virus es pequeño de tal modo no tengan un impacto negativo en el

MUNICIPALIDAD DE MIRAFLORES
JAVIER CONSTANTINO CARRANZA VERAMENDI
Gerente
V°B°
Gerencia de Sistemas y Tecnologías de la Información

		tráfico de la red (máximo 100Kb por actualización). ▪ La actualización de nuevas versiones del producto se pueden realizar automáticamente y no requiere la desinstalación y/o reinstalación de algún componente previo, estas actualizaciones son incrementales. ▪ La solución permite programar la comprobación de nuevas versiones de la solución al menos cada 12 horas y programar la instalación automática de ellas en horas de menos tráfico de red. Para este fin, la solución debe contar con opciones para la programación del horario por día y hora específica.
14	Consola de administración	▪ La solución deberá contar con una Consola de Administración Centralizada desde donde se pueda Administrar y controlar todos los componentes de la solución ofertada en forma centralizada y distribuida. ▪ La herramienta deberá tener incluido la capacidad de gestión de las políticas de Control de Acceso a la Red sin requerir instalar productos adicionales. ▪ La consola debe permitir la administración simultánea de equipos y servidores Windows, Linux y Mac. ▪ La herramienta deberá ser escalable y debe permitir la administración de complejas redes, permitiendo la administración centralizada y distribuida de más de 550 equipos desde una sola consola. ▪ La consola debe sincronizarse con el Directorio Activo para la instalación automática de la solución de seguridad en los equipos. ▪ La administración deberá estar basada en Políticas y debe contener al menos políticas para Actualización, Opciones Anti-Malware, HIPS, Control de Aplicaciones, Control de Dispositivos, Control de Fuga de Datos, NAC y Firewall. Cualquier cambio en las políticas deberán desplegarse automáticamente a los equipos sean estos Windows, Linux o Mac. ▪ Debe contar con filtros de control que permitan detectar de forma rápida los equipos no protegidos o los que no cumplen con las políticas de seguridad. ▪ El administrador deberá poder crear políticas desde la consola para evitar el uso de aplicaciones no deseadas así como eliminar, autorizar y limpiar las mismas en los clientes. ▪ La consola deberá poder utilizar al menos 3 tipos diferentes de mecanismos para detectar equipos en la red (TCP/IP, Active Directory y otros). ▪ Se deberá poder crear políticas de actualización para equipos con conexión lenta pudiendo limitarse el ancho de banda utilizado durante las actualizaciones.

MUNICIPALIDAD DE MIRAFLORES
JAVIER CONSTANTINO CARRANZA VERAMENDI
Gerente
V°B°
Gerencia de Sistemas y Tecnología de la Información

		▪ La consola deberá ser capaz de determinar equipos que cumplen con las políticas centrales y/o que fueron modificadas localmente. Eventualmente deberá poder "forzar" a los equipos a cumplir con las políticas centrales con tan solo un clic. ▪ La consola deberá contar con un sistema de reportes y mecanismos de notificación de eventos vía correo electrónico. ▪ La consola deberá almacenar un histórico de eventos de cada equipo administrado pudiéndose conocer también el Nombre del Equipo, Descripción, SO, Service Pack, IP, Grupo, Última Actualización, Eventos de error, etc. desde la consola. ▪ La consola deberá administrar el sistema de prevención contra intrusiones de hosts (HIPS) y el sistema de protección contra desbordamiento de buffers (BOPS) como políticas de seguridad. ▪ La consola deberá permitir delegar la administración basada en roles y ubicaciones geográficas, permitiendo de esta forma delegar la administración por áreas geográficas manteniendo de esta forma el control de la seguridad corporativa. ▪ El sistema para la delegación de roles deberá contener un administrador de permisos, pudiendo crear distintos perfiles con permisos particulares para cada administrador. ▪ La consola deberá permitir crear excepciones para el control de dispositivos (control total, solo lectura y bloqueo), filtrado URL (por nombre, IP's o Rango de IP's) para un grupo particular de equipos o toda la red. ▪ Debe incluir la capacidad para la desinfección y limpieza remota de adware/aplicaciones potencialmente peligrosas, así como también de virus, troyanos, gusanos, rootkits y Spyware. ▪ La consola deberá permitir acceder a un sistema de visualización y búsqueda de eventos para las políticas de control de aplicaciones, dispositivos, fuga de datos y firewall. ▪ La consola deberá tener integrada un Visor de Parches con la finalidad de que el administrador de la solución pueda verificar la lista de parches que faltan aplicar en los equipos administrados así como conocer la cantidad de equipos a los cuales falta aplicar un determinado parche. *Para demostrar el cumplimiento de esta característica el postor deberá adjuntar una captura de pantalla donde se muestre el cumplimiento de este requerimiento.* ▪ Desde el sistema de visualización y búsqueda de eventos se deberá poder generar Excepciones a las políticas de seguridad y control previamente establecidas.
15	Defensa en el Gateway y Servidor de Correo	▪ Se requiere una solución del mismo fabricante que brinde

MUNICIPALIDAD DE MIRAFLORES
JAVIER CONSTANTINO CARRANZA VERAMENDI
Gerente
V°B°
Gerencia de Sistemas y Tecnologías de la Información

		Seguridad y Control de la información entrante y saliente de la red vía los protocolos SMTP el cual deberá incluir su propio motor MTA. ▪ El postor deberá incluir la licencia que cubra el mantenimiento y actualización de un appliance físico y/o appliance virtual que funcionen como Gateway de Correo en modo de alta disponibilidad y cluster; así como proteger todos los servidores de correo de la institución en plataformas Linux (Zimbra), Windows (Exchange) y Lotus Domino. *El postor deberá señalar adjuntar información específica de cada producto que cubre este requerimiento.* ▪ La solución propuesta deberá rastrear, limpiar y eliminar virus, adware, spyware, aplicaciones potencialmente peligrosas y SPAM en dichos protocolos, en el Gateway y en los servidores de correo de la institución. ▪ *El postor deberá incluir la licencia para cada uno de los productos de protección de los servidores de correo y defensa en el Gateway perimetral para al menos 550 usuarios en cada caso según lo descrito líneas arriba.* **GATEWAY Y SERVIDOR DE CORREO (Protocolo SMTP)** ▪ Deberá contar con un sistema de Administración Seguro vía Web (HTTPS). ▪ Desde el sistema de administración se debe tener acceso a: La creación de políticas entrantes y salientes, listas blancas y negras personales y globales, reportes, sistema de solicitud de soporte, cuarentenas, etc. ▪ La solución deberá poder configurarse como Relay del correo electrónico y como servidor de correo en plataformas Linux. Así mismo deberá incluir versiones para proteger los servidores de correo interno de la institución como Exchange, Notes, Sendmail/Postfix frente a virus y spam generados internamente. ▪ La solución para el Gateway de correo deberá incluir el soporte para sistemas de archivamiento de correo y para la encriptación de mensajes. ▪ Deberá integrarse con el protocolo LDAP y Directorio Activo para la autenticación de usuarios y creación de políticas. ▪ Deberá incluir un filtro Anti Spam del mismo fabricante que soporte descargas automáticas de políticas anti spam. Deberá incluir varias técnicas de detección, como reputación de IP, heurística avanzada, huellas de mensajes y adjuntos, análisis de palabras clave, detección de direcciones web, etc. ▪ El producto debe tener una efectividad de detección de SPAM fuera de caja de un mínimo del 98%. Deberá entregarse información del fabricante para certificar esta funcionalidad. ▪ Deberá ofrecer una tecnología del mismo fabricante que permita el acceso en tiempo real a una amplia gama de

MUNICIPALIDAD DE MIRAFLORES - Gerencia de Sistemas y Tecnología de la Información
JAVIER CONSTANTINO CARRANZA VERAMENDI
Gerente
V°B°

		información reciente contra spam. Este sistema es conocido como Sistema de Protección Anti-Spam en tiempo real. El postor deberá incluir un gráfico donde se muestre el funcionamiento de esta característica. ▪ Deberá detectar ataques de robo de información (phishing), ataques de denegación de servicio (DoS) y cosecha de información (Harvest). ▪ Deberá contar con un sistema de protección contra robo de información que permita filtrar los mensajes buscando palabras definidas tanto en el mensaje como en los adjuntos del correo. ▪ Deberá contar con un módulo específico para el Filtrado por Reputación que permite el bloqueo por IP's de servidores dudosos y permitir elaborar excepciones tanto a nivel MTA como a nivel de políticas de correo. Esta lista deberá residir en el servidor y deberá ser actualizado en promedio cada 10 minutos y en forma incremental. ▪ Deberá soportar el sistema SPF (Sender Policy Framework) para evitar entrada de correo falsificado, así como tambien, deberá soportar el sistema de autenticación de correos conocido como DomainKeys. ▪ Deberá de poder detectar, eliminar y limpiar virus y spyware en los archivos adjuntos al correo electrónico y en el cuerpo del mensaje y deberá ser del mismo fabricante. ▪ Deberá de realizar el bloqueo de archivos adjuntos según el tipo de archivo y no de la extensión. ▪ Deberá de realizar el bloqueo de correos por asuntos, destinatario o texto en el cuerpo del mensaje. ▪ Deberá contar con un Editor de Políticas para filtrar el contenido del tráfico entrante y saliente. ▪ Deberá contar con opciones para realizar pruebas de las políticas creadas antes que estas entren a producción y emitir reportes de fallos y correcciones que deben realizarse. ▪ Deberá de poder hacer reglas de filtrado por usuario. ▪ Deberá de poder hacer creaciones de lista de aceptación y negación (blanca y negra) de dominios y usuarios (cuentas de correo) confiables. ▪ Deberá de enviar notificaciones configurables al emisor, receptor y al administrador sobre mensajes electrónicos infectados y/o bloqueados. ▪ Debe permitir crear usuarios para la administración basada en roles para delegar ciertas funcionalidades de administración. El acceso a la interfaz de administración basada en roles debe ser vía web seguro y debe funcionar en un puerto distinto al del Administrador principal. ▪ Deberá contar con un administrador de cuarentena central

MUNICIPALIDAD DE MIRAFLORES
JAVIER CONSTANTINO CARRANZA ERAMENDI
Gerente
V°B°
Gerencia de Sistemas y Tecnologías de la Información

		a nivel de consola. ▪ Deberá contar con un administrador de la cuarentena por usuario que permita a su vez administrar la lista blanca y negra de cada usuario. ▪ Debe poder desactivarse ciertas opciones a las cuales no se desea que los usuarios tengan acceso. ▪ Deberá contar con un sistema automático que permita realizar el backup de la cuarentena. Esta opción es configurable desde la herramienta de gestión del producto. ▪ Deberá generar un mensaje donde les informe a los usuarios finales los mensajes de correo puestos en cuarentena y que estos puedan recuperar todos o individualmente tan sólo con un solo clic. ▪ La herramienta debe contar con un sistema de actualización de cada parte de los componentes del producto incorporado en la herramienta de administración web. ▪ La herramienta deberá soportar la autenticación SMTP antes del envío y deberá poder integrarse con sistemas LDAP y Directorio Activo para realizar esta función. El postor deberá presentar la captura de pantalla donde se muestre la forma de funcionamiento de esta característica. ▪ Los equipos appliances deberán funcionar en modo activo-pasivo y con sincronización automática de la configuración y políticas. Así mismo deberá soportar el balanceo de carga. ▪ No deberá requerirse la instalación de script's ni productos de terceros para el funcionamiento del producto.
16	Administración de Licencias	▪ La solución debe permitir el manejo flexible de las licencias, de manera que puedan ser reasignadas en caso se cambie de equipo. ▪ La licencia del software propuesto deberá permitir el Uso de la solución antivirus en una pc's de casa de los trabajadores de la institución hasta un máximo del número de licencias adquiridas. ▪ Para certificar el cumplimiento de este requerimiento el Postor deberá adjuntar una copia del Contrato de Uso de la Licencia del producto propuesto donde se señale este requerimiento.
ATRIBUTOS DE USO		
17	Alertas y Reportes	▪ La solución deberá ser capaz de notificar los eventos de virus a través de diferentes medios (correo electrónico, alertas de registros, etc.) ▪ La solución deberá generar reportes gráficos, imprimibles y exportables de la cobertura de versiones, actualizaciones e infecciones. ▪ La solución deberá contener un sistema de reportes que

MUNICIPALIDAD DE MIRAFLORES
JAVIER CONSTANTINO CARRANZA ERAMENDI
Gerente
V°B°
Gerencia de Sistemas y Tecnologías de la Información

		permite ver el estado de la protección de la red en línea. Este sistema debe mostrar en tiempo real lo que está ocurriendo en la red. ▪ La solución deberá permitir acceder a reportes basados en el usuario que permita conocer rápidamente el cumplimiento de políticas por cada usuario. ▪ La solución deberá incorporar un sistema de reportes que permita programar la creación y envío de reportes en formato PDF y HTML vía correo en una determinada hora y fecha del día. ▪ La solución deberá incorporar un mecanismo de conexión con la base de datos para la creación de reportes personalizados y directos a la base de datos.
18	Soporte técnico	▪ La solución debe contar con soporte técnico 24/7 escalable hacia la casa matriz incluido en la licencia y en español. *El postor deberá presentar un documento del fabricante donde certifique que cuenta con este tipo de soporte.* ▪ Si para el escalamiento se requiere de un código especial para el soporte desde la casa matriz el postor deberá especificarlo mediante una declaración jurada comprometiéndose a brindar dicho código el cual deberá ser emitido a nombre de la ENTIDAD al momento de la firma del contrato. ▪ El fabricante de la solución deberá contar con el soporte remoto local bajo demanda y sin costo durante todo el periodo de licenciamiento. Para usar este sistema no deberá requerirse instalar ningún software en el equipo cliente ni realizar cambios en la configuración de la red. El postor deberá detallar en su propuesta incluyendo características y capturas de pantallas del funcionamiento de su sistema de soporte remoto bajo demanda. ▪ El Postor deberá contar con al menos dos Especialistas Certificado por el fabricante en las áreas de Antivirus, Antispam y Control de Acceso a la Red. *El postor deberá incluir los certificados emitidos.* ▪ El postor capacitará un mínimo de 10 horas en las herramientas administrativas del software dictado y certificado por el Postor, para 5 personas como mínimo, el mismo que debe ser dictado dentro de los quince días hábiles posteriores a la fecha de recepción e instalación. ▪ El postor deberá brindar el servicio de instalación, configuración y pruebas del aplicativo antivirus en el 50% de equipos de la institución. ▪ El postor tendrá 30 días calendarios para realizar la implementación en los equipos señalados líneas arriba contabilizados desde el día siguiente de colocada la orden de compra. ▪ El postor deberá adjuntar obligatoriamente a su propuesta técnica, toda la documentación técnica necesaria y copias

MUNICIPALIDAD DE MIRAFLORES
JAVIER CONSTANTINO CARRANZA VERAMENDI
Gerente
V°B°
Gerencia de Sistemas y Tecnologías de la Información

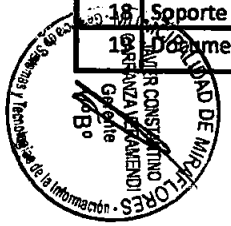
		de la certificación ICSA Labs para efectos de ser sometidos a evaluación técnica. ▪ El fabricante deberá contar con un tiempo de respuesta ante nuevos malwares como máximo de 4 horas el cual deberá estar validado por el estudio realizado por AV-Test.org. *Para certificar esta característica el postor deberá adjuntar a su propuesta técnica una copia del documento para efectos de ser sometidos a evaluación técnica.*
19	Documentación	▪ La solución deberá contar con todos los manuales que permitan su instalación y configuración. ▪ Se deberá incluir manuales de instalación paso a paso de toda la solución instalada en la institución.

MUNICIPALIDAD DE MIRAFLORES
JAVIER CONSTANTINO CARRANZA VERAMENDI
Gerente
V°B°
Gerencia de Sistemas y Tecnologías de la Información

7. Análisis comparativo técnico

Se ha establecido la siguiente escala para la valoración de cada atributo definido en el punto 6.3:

Modelo de Calidad		Escala	Productos Evaluados		
Item	Atributo	Puntaje Máximo	KASPERSKY Kaspersky Open Space	SOPHOS Endpoint + Email Security and Control	PANDA Panda Cloud Protection
ATRIBUTOS INTERNOS					
1	Sistemas operativos de estaciones de trabajo	5	5	5	5
2	Sistemas operativos de servidores de red	3	3	3	3
3	Protección y defensa frente a malware en portátiles, computadoras de escritorio y servidores.	7	7	7	7
4	Firewall	3	3	3	3
5	Sistema de prevención de intrusos de hosts – HIPS y detección de desbordamiento de buffers (BOPS – Buffer Overflow Protection System)	4	2	4	2
6	Control de dispositivos	5	4	5	3
7	Protección contra ataques de día cero.	4	4	4	4
8	Seguridad	4	4	4	4
9	Control de aplicaciones	5	2	5	2
10	Control de acceso a la red	5	2	5	2
11	Control de fuga de información(DLP)	7	4	7	2
ATRIBUTOS EXTERNOS					
12	Instalación y despliegue del software	5	4	5	5
13	Actualización de firmas y nuevas versiones del producto.	5	5	5	5
14	Consola de administración	8	7	8	8
15	Defensa en el Gateway y Servidor de Correo	10	6	10	9
16	Administración de Licencias	5	5	5	5
ATRIBUTOS DE USO					
17	Alertas y Reportes	5	5	3	5
18	Soporte técnico	5	5	5	5
19	Documentación	5	5	5	5
		100	82	98	84



8. Análisis comparativo costo-beneficio

8.1. Costo

El presente documento tiene la finalidad de obtener las mejores características técnicas disponibles en el mercado para la solución que requiere la Municipalidad por lo que la obtención del costo no es materia del presente. Sin embargo, de acuerdo a los procedimientos administrativos la obtención del precio referencial será realizado previa a la convocatoria y corresponde al área responsable realizar el análisis de costo respectivo.

8.2. Beneficio

La SOFTWARE ANTI-VIRUS, ANTI-SPAM Y CONTROL DE ACCESO A LA RED brindará protección contra malware, spyware, adware y otras amenazas a las estaciones de trabajo y servidores; así como también permitirá controlar el riesgo de que se afecte la integridad de la información y el normal desarrollo de las actividades de la institución mediante la protección a nivel perimetral de las comunicaciones de la institución.

9. Conclusiones

- El presente informe, identifica las características técnicas mínimas obligatorias y deseables para la adquisición de la solución integral corporativa de antivirus.

10. Firmas de los responsables de la evaluación

Responsable de la evaluación	Firma
Javier Vílchez López	

MUNICIPALIDAD DE MIRAFLORES
JAVIER CONSTANTINO CARRANZA VERAMENDI
Gerente
V°B°
Gerencia de Sistemas y Tecnologías de la Información