INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE N°044-2013-GIN/SAT

1. **NOMBRE DEL ÁREA:**

   Gerencia de Informática

2. **RESPONSABLES DE LA EVALUACIÓN:**

   Cesar Terry Ramos

3. **CARGO:**

   Jefe de División de Soporte y Producción.

4. **FECHA DE APROBACION**

   05 de marzo del 2013

5. **JUSTIFICACIÓN**

   El Servicio de Administración Tributaria SAT Lima, requiere la adquisición de software anual de 730 Licencias de antivirus con funciones de anti-spam y control de acceso a la red, para la protección de equipos informáticos.

   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 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 los recursos de la red, identificando las amenazas o debilidades de la infraestructura de red, ayudando inmediatamente a tomar acciones (prevención de 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 de funciones de 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, sin requerir el cambio de dichos equipos bajo ningún concepto.

   De acuerdo a Ley es necesario evaluar programas de software que cumplan con las especificaciones técnicas requeridas, independientemente del que se ha venido utilizando a la fecha, y a fin de proceder a su adquisición en un número igual.

SAT Servicio de Administración Tributaria de Lima
CESAR TERRY RAMOS
JEFE DE DIVISION DE SOPORTE Y PRODUCCION

6. ALTERNATIVAS.

Se analizaron los siguientes productos antivirus:

- McAfee
- Sophos
- Symantec

7. ANALISIS COMPARATIVO TÉCNICO

Se procedió en aplicación de la parte 3 de la Guía de Evaluación de Software aprobada por Resolución Ministerial Nº 139-2004-PCM:

a. Propósito de la Evaluación:

- Determinar los atributos o características mínimas para el Producto Final Software de Antivirus con funciones de Anti-Spam y Control de Acceso a la Red.

b. Identificar el tipo de producto

- Software de Antivirus Servidor Cliente

c. Especificaciones del Modelo de Calidad

- Se aplica al Modelo de Calidad de Software descrito en la Parte I de la Guía de Evaluación de Software aprobado por Resolución Ministerial No 139-2004-PCM.

d. Selección de Métricas

- Las métricas fueron seleccionadas en base al análisis de los requerimientos del área usuaria y a la información técnica de los productos de Software de Antivirus con funciones de Anti-Spam y Control de Acceso a la Red señalados en el punto "6. ALTERNATIVAS"

Del análisis realizado, se han determinado las siguientes características técnicas mínimas y sus respectivas métricas.

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 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 2003 Server ▪ Microsoft Windows 2008 Server ▪ Red Hat Enterprise 4/5/6 En versiones de 32 y 64 bits.

SAT Servicio de Administración Tributaria de Lima
CESAR TERRY RAMOS
JEFE DE DIVISION DE SOPORTE Y PRODUCCION

3	Protección y defensa frente a malware.	▪ 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 reportes publicados por dicha compañía. ▪ 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, etc) donde le indique al usuario la razón por la que no ha podido acceder a dicha página. ▪ La solución deberá incluir un sistema para el Control de acceso web a sitios inapropiados. Este sistema deberá estar integrado al agente antimalware y deberá permitir, notificar o bloquear el acceso a sitios web en base a categorías. ▪ La solución para el Control de acceso a web a sitios inapropiados deberá incluir al menos 10 categorías de sitios web entre las que se encuentren principalmente Actividad Criminal, Armas, Contenido Ofensivo, Contenido para adultos, Juegos de Azar, Robo de Datos y Fraude, Programas Espía, Proxys anónimos, Violencia y Hackers. ▪ La solución cuenta con la Certificación por la detección de programas espía. ▪ 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.

SAT Servicio de Administración Tributaria de Lima
CESAR TERRY RAMOS
JEFE DE DIVISION DE SOPORTE Y PRODUCCION

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 debe reconfigurar con otro tipo de política de protección de acuerdo a la ubicación donde se encuentre. Esta reconfiguración deberá realizarse 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.
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

SAT Servicio de Administración Tributaria de Lima
CESAR TERRY RAMOS
JEFE DE DIVISION DE SOPORTE Y PRODUCCION

		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. ▪ 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. ▪ Cualquier intento de vulneración de las características de seguridad deberá ser reportado a la Consola de Gestión Centralizada..

SAT Servicio de Administración Tributaria de Lima
CESAR TERRY RAMOS
JEFE DE DIVISION DE SOPORTE Y PRODUCCION

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 categorizadas por tipo de programas; al menos como Programas P2P, Mensajería, Proxy's, Herramientas de Hacking, Control Remoto de Equipos y Máquinas Virtuales. ▪ La solución permite limpiar y desinstalar remotamente las principales aplicaciones P2P controladas (Peer-to-peer) desde la Consola de Administración. ▪ La entidad puede solicitar al fabricante y/o distribuidor 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 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.
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 políticas corporativas.

SAT Servicio de Administración Tributaria de Lima
CESAR TERRY RAMOS
JEFE DE DIVISION DE SOPORTE Y PRODUCCION

		▪ 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 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 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.

SAT Servicio de Administración Tributaria de Lima
CESAR TERRY RAMOS
JEFE DE DIVISION DE SOPORTE Y PRODUCCION

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 y Linux . ▪ La herramienta deberá ser escalable y debe permitir la administración de redes complejas, permitiendo la administración centralizada y distribuida de más de 800 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 y Linux. ▪ 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. ▪ 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

SAT
Servicio de Administración Tributaria de Lima
CESAR TERRY RAMOS
JEFE DE DIVISION DE SOPORTE Y PRODUCCION

		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. ▪ La consola deberá tener integrado un Visor para el Control web el cual deberá permitir visualizar los sitios web a los cuales los usuarios han intentado ingresar en contra de las políticas de seguridad de la empresa. ▪ Desde el sistema de visualización y búsqueda de eventos se deberá poder generar Excepciones a las políticas de seguridad y control previamente establecidas.
15	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.
ATRIBUTOS DE USO		
16	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.

SAT Servicio de Administración Tributaria de Lima
CESAR TERRY RAMOS
JEFE DE DIVISION DE SOPORTE Y PRODUCCION

		▪ La solución deberá contener un sistema de reportes que 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.
17	Soporte técnico	▪ La solución debe contar con soporte técnico 24/7 escalable hacia la casa matriz incluido en la licencia y en español. ▪ Si para el escalamiento se requiere de un código especial para el soporte desde la casa matriz se deberá especificar el procedimiento. ▪ 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.
18	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.

e. Niveles, escalas para las métricas.

Determinar las características técnicas mínimas y las métricas aplicables, se procedió al análisis comparativo técnico, para lo cual se aplico el Modelo de Calidad de Software descrito en la Parte I de la Guía Evaluación de Software por Resolución Ministerial No 139-2004-PCM.

Escalas	Siglas	Descripción
Muy Bueno	MB	Cumple con todas las características técnicas obligatorias y todas las deseables.
Bueno	B	Cumple con todas las características técnicas obligatorias y alguna de las deseables.
Pobre	P	Cumple con algunas de las características técnicas obligatorias y/o deseables.
No aceptable	NA	No cumple con las características técnicas obligatorias.

f. Se ha establecido la siguiente escala para la valoración de cada atributo definido en el punto "e":

SAT Servicio de Administración Tributaria de Lima
CESAR TERRY RAMOS
JEFE DE DIVISION DE SOPORTE Y PRODUCCION

Modelo de Calidad		Escala	Productos Evaluados		
Item	Atributo	Puntaje Máximo	MCAFEE Total Protection for Secure Business	SOPHOS Endpoint Security and Control	SYMANTEC Protection Suite Enterprise Edition
ATRIBUTOS INTERNOS					
1	Sistemas operativos de estaciones de trabajo	**MB**	MB	MB	MB
2	Sistemas operativos de servidores de red	**MB**	MB	MB	MB
3	Protección y defensa frente a malware	**MB**	B	MB	B
4	Firewall	**MB**	MB	MB	MB
5	Sistema de prevención de intrusos de hosts – HIPS y detección de desbordamiento de buffers (BOPS – Buffer Overflow Protection System)	**MB**	B	MB	B
6	Control de dispositivos	**MB**	MB	MB	MB
7	Protección contra ataques de día cero.	**MB**	MB	MB	MB
8	Seguridad	**MB**	MB	MB	B
9	Control de aplicaciones	**MB**	B	MB	B
10	Control de acceso a la red	**MB**	MB	MB	MB
11	Control de fuga de información(DLP)	**MB**	MB	MB	B
ATRIBUTOS EXTERNOS					
12	Instalación y despliegue del software	**MB**	MB	MB	MB
13	Actualización de firmas y nuevas versiones del producto.	**MB**	B	MB	B
14	Consola de administración	**MB**	B	MB	B
15	Administración de Licencias	**MB**	MB	MB	MB
ATRIBUTOS DE USO					
16	Alertas y Reportes	**MB**	MB	MB	MB
17	Soporte técnico	**MB**	MB	MB	MB
18	Documentación	**MB**	MB	MB	MB

SAT Servicio de Administración Tributaria de Lima
CESAR TERRY RAMOS
JEFE DE DIVISION DE SOPORTE Y PRODUCCION

8. ANALISIS COMPARATIVO TÉCNICO

Costo

El presente documento tiene la finalidad de obtener las mejores características técnicas disponibles en el mercado para la solución que requiere nuestra entidad, 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.

Beneficio

El Software Antivirus con funciones de AntiSpam y Control de Acceso a la Red, brindará protección contra malware, spyware, adware y otras amenazas a las estaciones de trabajo; 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

CESAR TERRY RAMOS
Jefe de Soporte y Producción
Servicio de Administración Tributaria