INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE Nº031-2011-GIN/SAT

1. **NOMBRE DEL ÁREA:**

   Gerencia de Informática

2. **RESPONSABLES DE LA EVALUACIÓN:**

   Cesar Edilberto Terry Ramos

3. **CARGO:**

   Jefe de División de Soporte y Producción.

4. **FECHA DE APROBACION**

   10 de enero del 2011

5. **JUSTIFICACIÓN**

   El Servicio de Administración Tributaria SAT Lima, requiere la adquisición de software anual de 600 Licencias de antivirus para la protección de equipos informáticos, como parte de la seguridad de red informática.

   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.

6. **ALTERNATIVAS**

   Se analizaron los siguientes productos antivirus:
   - McAfee Endpoint Protection Advanced Suite
   - Sophos Endpointl Security and Control
   - Symantec Endpoint Protection 11.0
   - Trend Micro OfficeScan™ Client/Server Edition

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.

   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 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)		
Ítem	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 incluida en el Cuadrante Mágico de Gartner de Plataformas de Protección de Punto Final como Líder en los últimos 2 reportes publicados por dicha compañía (2008 y 2009). 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. La solución cuenta con la Certificación Checkmark Checkmark 100% 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.
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 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.	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 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. 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 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 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 tráfico de la red (máximo 100Kb por actualización). La actualización de nuevas versiones del producto se puede 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 500 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. 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. 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. 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		
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.

		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.
17	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 el certificado emitido. El postor capacitará un mínimo de 5 horas en las herramientas administrativas del software dictado y certificado por el Postor, para 04 personas como mínimo por cada institución, 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 los equipos de la institución.

		El postor deberá adjuntar obligatoriamente a su propuesta técnica, toda la documentación técnica necesaria y copias 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.
18	Documentación	Obligatorios 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.

Ítem	Atributo	Puntaje Máximo
1	Sistemas operativos de estaciones de trabajo	5
2	Sistemas operativos de servidores de red	5
3	Protección y defensa frente a malware en portátiles, computadoras de escritorio y servidores.	6
4	Firewall	4
5	Sistema de prevención de intrusos de hosts – HIPS y detección de desbordamiento de buffers	8
6	Control de dispositivos	7
7	Protección contra ataques de día cero.	7
8	Seguridad	6
9	Control de aplicaciones	6
10	Control de acceso a la red	8
11	Control de fuga de información(DLP)	6
12	Instalación y despliegue del software	3
13	Actualización de firmas y nuevas versiones del producto.	5
14	Consola de administración	6
15	Administración de Licencias	2
16	Alertas y Reportes	4
17	Soporte técnico	7
18	Documentación	5
	PUNTAJE TOTAL	100

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.

Ítem	Atributo	Puntaje Máximo	McAfee	Sophos	Symantec	Trend Micro
1	Sistemas operativos de estaciones de trabajo	5	5	5	5	5
2	Sistemas operativos de servidores de red	5	5	5	5	5
3	Protección y defensa frente a malware en portátiles, computadoras de escritorio y servidores.	6	6	6	6	6
4	Firewall	4	4	4	4	4
5	Sistema de prevención de intrusos de hosts – HIPS y detección de desbordamiento de buffers	8	6	7	7	6
6	Control de dispositivos	7	6	7	6	5
7	Protección contra ataques de día cero.	7	6	7	6	7
8	Seguridad	6	6	6	6	6
9	Control de aplicaciones	6	6	6	6	5
10	Control de acceso a la red	8	7	7	7	4
11	Control de fuga de información(DLP)	6	4	6	4	4
12	Instalación y despliegue del software	3	3	3	3	3
13	Actualización de firmas y nuevas versiones del producto.	5	5	5	5	5
14	Consola de administración	6	6	6	6	6
15	Administración de Licencias	2	2	2	2	2
16	Alertas y Reportes	4	4	3	4	4
17	Soporte técnico	7	7	7	7	7
18	Documentación	5	5	5	5	5
	Puntaje Total	100	93	97	94	89

8. ANALISIS COMPARATIVO DE COSTO - BENEFICIO

Licenciamiento:

Se requiere la adquisición de seiscientas (600) licencias de software de Antivirus para protección de los equipos informáticos.

Mantenimiento:

La adquisición de las licencias de software, debe considerar la suscripción anual de soporte y mantenimiento.

Se ha realizado el análisis comparativo de costos de los productos señalados en el punto 6: ALTERNATIVAS.

Producto	Fabricante	No Licencias	Precio Unit.	Total	Total IGV
McAfee Endpoint Protection Advanced	McAfee	600	55.51	IGV Incluido	33,306.60
Sophos Endpoint Security and Control	Sophos	600	54.33	IGV Incluido	32,600.00
Symantec endpoint protection	Symantec	600	57.78	IGV Incluido	34,671.00

Hardware:

Estos productos se adaptan y son compatibles con la plataforma informática de Hardware.

Beneficios:

Los Beneficios obtenidos a partir de la implementación del uso del software de Antivirus, sobre la plataforma de equipos informáticos, han sido entre otros:

- Reducción de las infecciones de equipos informáticos, en tiempo real.
- Centralización y automatización de las instalaciones locales y remotas.
- Proliferación de infecciones causadas a través de correo no deseado.
- Soporte Técnico las 24 horas del día.

9. CONCLUSIONES

Se determinaron los atributos o características técnicas que deben ser consideradas en la evaluación del software de Antivirus, estableciéndose la valoración de cada característica dentro del modelo descrito en la Parte de la Guía de Evaluación de Software aprobado por resolución Ministerial No 139-2004-PCM.

De acuerdo a los tramites comparativos técnicos y económicos, se ha podido determinar que el software de la firma Sophos, Producto: Endpoint Security and Control, cumple como la mejor alternativa para la protección de seguridad informática.

10. FIRMAS

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