SUNAT

**INFORME TECNICO PREVIO DE EVALUACIÓN DE SOFTWARE N° 002-2011/2A2000**

## 1. NOMBRE DEL AREA:

OFICINA DE INVESTIGACIÓN Y TECNOLOGIA

## 2. RESPONSABLES DE LA EVALUACION:

VICENTE RAUL TAPIA DIAZ

## 3. CARGO:

PROFESIONAL DE LA OFICINA DE INVESTIGACIÓN TECNOLOGICA

## 4. FECHA

11 DE MARZO DEL 2011

## 5. JUSTIFICACIÓN

La institución requiere contar con una herramienta integrada que ofrezca una solución antivirus, tanto para las estaciones de trabajo como para los servidores es decir, al total de equipos del parque informático institucional; abarcando de este modo las estaciones de trabajo, servidores de archivos, servidores de correo, logrando la protección permanente contra virus informáticos en cualquier punto de la red corporativa, permitiendo además una administración de políticas y generación de informes centralizadas a través de una única consola administrativa.

## 6. ALTERNATIVAS

Se analizaron las siguientes herramientas antivirus:

- McAfee Endpoint Protection Suite, que en adelante se le llamará McAfee
- SOPHOS Endpoint Security and Control 9.7 + Sophos Email Security For Exchange, que en adelante se le llamará Sophos
- Kaspersky Enterprise Space Security R2 MP4, que en adelante se le llamará Kaspersky

## 7. ANALISIS COMPARATIVO TECNICO

Para cada uno de los productos seleccionados se han evaluado los atributos que conforman el requerimiento técnico mínimo que la herramienta debe cumplir, en el siguiente cuadro se muestran los puntajes máximo y mínimo de cada atributo:

INTENDENCIA NACIONAL DE SISTEMAS DE INFORMACION
Oficina de Investigación y Tecnología
JEFE (e)
DAMASO CARLOS TAY

**REQUERIMIENTO MÍNIMO:**

| | Puntaje Máximo | McAfee | Sophos | Kaspersk |
|---|---|---|---|---|
| **PUNTAJE TOTAL** | **100** | **100** | **99** | **100** |
| **ATRIBUTOS INTERNOS** | **30** | **30** | **30** | **30** |
| **Funcionalidad: Adecuación**<br>Sistemas Operativos soportados de las estaciones de trabajo Windows XP, Windows Vista, Windows 7. | 3 | 3 | 3 | 3 |
| **Funcionalidad: Adecuación**<br>Soporte de Servidores de Archivos. Soporte a los Sistemas Operativos MS Windows Server 2003 y MS Windows Server 2008. El soporte será brindado a todas las Ediciones de los productos. | 3 | 3 | 3 | 3 |
| **Funcionalidad: Adecuación**<br>Compatibilidad con servidores de Mensajería Electrónica MS Exchange Server 2003, Exchange Server 2007. | 3 | 3 | 3 | 3 |
| **Funcionalidad: Seguridad**<br>Detecta en tiempo real cualquier archivo infectado que trate de ser ejecutado, leído, copiado hacia/desde el servidor/estación de trabajo. El código malicioso debe ser detenido antes de que pueda propagarse por la red. | 3 | 3 | 3 | 3 |
| **Funcionalidad: Seguridad**<br>Da soluciones en forma inmediata a todas las nuevas tecnologías de códigos maliciosos existentes: gusanos, troyanos, virus encriptables, stealth, tunneling, polimórficos, Multipropósito, macrovirus (Word, Excel, PowerPoint), virus de Java, JavaScripts, Visual Basic, script, html, Corel, y nuevas tecnologías de virus no identificadas aún, comprometiéndose el postor en eliminar de forma inmediata estas amenazas. | 3 | 3 | 3 | 3 |
| **Funcionalidad: Seguridad**<br>Posibilidad de búsqueda en recursos de red compartidos, rastreo de virus en los discos de los usuarios, los disquetes u otras unidades de almacenamiento removibles. | 3 | 3 | 3 | 3 |
| **Fiabilidad: Madurez**<br>Permite bloquear una amplia gama de amenazas de virus y código malicioso, usando heurística avanzada y detección genérica para ofrecer protección incluso ante amenazas nuevas y desconocidas, resguardando los equipos contra exploits. | 3 | 3 | 3 | 3 |
| **Fiabilidad: Madurez**<br>Detección y categorización de nuevas amenazas expandidas como Spyware y Adware. | 3 | 3 | 3 | 3 |
| **Fiabilidad: Madurez**<br>Permite bloquear puertos de comunicación para combatir epidemias. Así como también crear políticas de denegación de escritura en forma centralizada. | 3 | 3 | 3 | 3 |
| **Fiabilidad: Madurez**<br>Ejecuta actualizaciones aleatorias de las firmas desde los clientes para evitar el congestionamiento de la red. | 3 | 3 | 3 | 3 |

INTENDENCIA NACIONAL DE SISTEMAS DE INFORMACIÓN
Oficina de Investigación Tecnológica
JEFE (e)
DAMASO CARLOS TAY

| | | | | |
|---|---|---|---|---|
| **ATRIBUTOS EXTERNOS** | **24** | **24** | **24** | **24** |
| **Funcionalidad: Adecuación**<br>Protegerá de manera específica los servidores de correo electrónico de los virus que pudieran ingresar al sistema en este nivel de la red, con soporte antivirus para servidores Microsoft Exchange Server (versiones 2010, 2007 y 2003) | 3 | 3 | 3 | 3 |
| **Funcionalidad: Adecuación**<br>Capacidad de escanear en tiempo real los datos adjuntos de correo electrónico mediante los protocolos estándares, y SMTP configurados en clientes de correo como MS Outlook. | 3 | 3 | 3 | 3 |
| **Funcionalidad: Exactitud**<br>Detección durante descarga de Archivos, el producto detecta y realiza la eliminación de código malicioso en archivos comprimidos. | 3 | 3 | 3 | 3 |
| **Funcionalidad: Exactitud**<br>Bloqueo de mensajes de correo electrónico no deseado, dependiendo del dominio remitente o de direcciones de correo independientes | 3 | 3 | 3 | 3 |
| **Funcionalidad: Exactitud**<br>Administración remota basada en Web (http o https), y/o una consola de gestión compatible a Microsoft, que se puede realizar en forma remota, desde cualquier estación de trabajo a través de un acceso seguro. | 3 | 3 | 3 | 3 |
| **Funcionalidad: Seguridad**<br>El producto bloquea al usuario a navegar involuntariamente en páginas peligrosas que contengan código malicioso cuando haga consultas en sitios de motores de búsquedas en línea (Google, Bing, etc). | 3 | 3 | 3 | 3 |
| **Funcionalidad: Seguridad**<br>Detección de virus durante la navegación en internet, permite navegar y buscar en la web de forma segura evitando amenazas como programas espía, programas publicitarios, phishing, estafas por robo de identidad, etc. | 3 | 3 | 3 | 3 |
| **Funcionalidad: Seguridad**<br>Bloquea los sitios con un número excesivo de menús emergentes, prácticas fraudulentas y aprovechamiento de debilidades, como el software publicitario y el software espía, así como enlaces ocultos a otros sitios web dañinos. | 3 | 3 | 3 | 3 |
| **ATRIBUTOS DE USO** | **46** | **46** | **45** | **46** |
| **Eficacia**<br>Las actualizaciones del producto podrán realizarse a través de un archivo instalable (descargado desde sitio en Internet) y distribuirse a través de la red corporativa; las actualizaciones a distribuir son solo incrementales. | 3 | 3 | 3 | 3 |
| **Eficacia**<br>Las actualizaciones deberán obtenerse directamente de los sitios disponibles por el fabricante en forma automática, y ser aplicadas a cada uno de los productos de la solución. | 4 | 4 | 4 | 4 |
| **Productividad**<br>Ejecuta reporte en formato gráfico, incluyendo reportes predeterminados, los eventos pueden consultarse accediendo a vistas publicas en el motor de base de | 3 | 3 | 3 | 3 |

JEFE (e)

| | | | | |
|---|---|---|---|---|
| datos (MSSQL Server 2005/2008, Ms SQL Express MSDE, 2005,2008) | | | | |
| **Productividad**<br>Permita crear reporte de infección, que permita identificar: equipo, usuario, nombre del archivo infectado, virus y acción realizada por el usuario. | 4 | 4 | 4 | 4 |
| **Productividad**<br>Permite ejecutar reportes individuales y personalizados, relacionados a equipos y archivos afectados. | 4 | 4 | 4 | 4 |
| **Seguridad**<br>La consola de administración mantiene una base de datos interna o externa (Deberá de soportar de forma mandataria MSDE, MS SQL y MySQL) en la cual se almacenará en tiempo real toda la información relacionada a la actividad en la plataforma de seguridad y antivirus (despliegue, instalación, actualización, monitoreo). | 4 | 4 | 3 | 4 |
| **Seguridad**<br>Protección a los usuarios contra el software dañino basado en la web: software publicitario, software espía, virus, estafas por robo de identidad, etc.; convirtiendo la navegación por la web en una actividad más segura. | 4 | 4 | 4 | 4 |
| **Seguridad**<br>Capacidad de auditorías de red para localizar equipos que no tengan instalada la herramienta antivirus, o se encuentre desactualizada. | 4 | 4 | 4 | 4 |
| **Satisfacción**<br>Permite realizar escaneos bajo demanda (ejecutados de manera remota por el administrador o a solicitud del usuario) a horas determinadas. | 4 | 4 | 4 | 4 |
| **Satisfacción**<br>Es utilizado como complemento de los navegadores MS Internet Explorer y deseable con Mozilla Firefox, Google Chrome | 4 | 4 | 4 | 4 |
| **Satisfacción**<br>Capacidad de escanear en tiempo real los datos adjuntos de correo electrónico mediante los protocolos estándares, y SMTP configurados en clientes de correo como MS Outlook. | 4 | 4 | 4 | 4 |
| **Satisfacción**<br>Capacidad de escanear virus y amenazas expandidas de los procesos que se estén ejecutando en memoria con la capacidad de terminar el proceso o darle manejo de acuerdo a las acciones previamente definidas. | 4 | 4 | 4 | 4 |

INTENDENCIA NACIONAL DE SISTEMAS DE INFORMACIÓN
Oficina de Investigación Tecnológica
JEFE (e)
DAMASO CARDENAS TAVARA

## ANALISIS COSTO - BENEFICIO

Licenciamiento: La herramienta McAfee tiene un costo estimado de S/. 619,375.68 y la garantía de buen funcionamiento por tres años tiene un costo de 74,325.24 lo que hace un total de S/. 693,700.92. La herramienta SOPHOS tiene un costo estimado de S/. 515,925.00 y la garantía de buen funcionamiento por tres años tiene un costo de S/. 128,520.00 lo que hace un total de S/. 644,445.00. La herramienta Kaspersky tiene un costo estimado de S/. 421,855.50 y la garantía de buen funcionamiento por tres años tiene un costo de S/. 42,186.00 lo que hace un

total de S/. 464,041.50. Estos costos incluyen el IGV y son para un total de 7,840 licencias, también incluyen la instalación, configuración, puesta en producción y capacitación.

Hardware necesario para su funcionamiento: SUNAT cuenta con los equipos necesarios para el correcto funcionamiento del software por lo que no es necesario realizar inversiones adicionales.

Soporte y mantenimiento externo: La cotización incluye una garantía por tres años la cual incluye: permanente actualización del software, el análisis, determinación, corrección y documentación de problemas de programas-producto instalados.

Personal: SUNAT cuenta con personal dedicado a la administración de la Arquitectura Informática, el cuál será entrenado para administrar la herramienta.

Capacitación: Dentro de los costos de licenciamiento se incluye la capacitación al personal que administrará la herramienta.

**BENEFICIO**:

El beneficio es disponer de una herramienta de protección contra los virus informáticos y evitar la pérdida de información por esta causa.

Evitar tiempos improductivos debido a la presencia de virus informático en los computadores.

## 8. CONCLUSIÓN

Las tres herramientas analizadas cumplen con los requisitos técnicos mínimos, por lo tanto, se recomienda realizar un proceso por concurso en la que participen estas herramientas, además de cualquier otra que satisfaga los requerimientos técnicos mínimos.

## 9. FIRMA