SUNAT

**INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE N° 011 / 2A2000**

1. **NOMBRE DEL AREA:**

   OFICINA DE INVESTIGACIÓN TECNOLÓGICA

2. **RESPONSABLES DE LA EVALUACION:**

   VICENTE RAÚL TAPIA DIAZ

3. **CARGO:**

   ANALISTA DE TECNOLOGÍA

4. **FECHA**

   19 DE DICIEMBRE DEL 2006

5. **JUSTIFICACIÓN**

   Es necesario disponer de una herramienta de protección contra ataques de virus informáticos tanto en los computadores personales de los trabajadores como el los servidores institucionales.

6. **ALTERNATIVAS**

   Se analizaron los siguientes productos:
   - McAfee Active Virus Defense.
   - Symantec AntiVirus
   - Kaspersky Corporate Suite

7. **ANALISIS COMPARATIVO TECNICO**

   Para cada uno de los productos seleccionados se han evaluado los atributos que mínimos que la solución debe contemplar, en el siguiente cuadro se muestran los puntajes máximo y mínimo de cada atributo:

| | Puntaje Mínimo | Puntaje Máximo | McAfee | Norton | Kaspersky |
|---|---|---|---|---|---|
| **PUNTAJE TOTAL** | 73 | 100 | | | |
| **ATRIBUTOS INTERNOS** | **13** | **20** | | | |
| **Acción multinivel de protección**<br>El software antivirus abarca las estaciones de trabajo, servidores de archivos, servidores de correo y el perímetro de Internet, de tal forma que se logre la protección permanente contra virus informáticos en cualquier punto de la red corporativa. | 2 | 3 | 3 | 3 | 3 |
| **Sistemas Operativos soportados de las estaciones de trabajo**<br>Windows95, Windows98, Windows2000 Professional, Windows XP, Windows Vista, Linux. | 1 | 2 | 2 | 2 | 2 |
| **Sistemas Operativos soportados de los servidores de red**<br>Microsoft Windows NT Server 4.0, Windows 2000 Server, Windows 2003 Server (todas las versiones), UNIX, HP UX, AIX, y Linux. | 1 | 2 | 2 | 2 | 2 |
| **Tipo de detección**<br>El software antivirus tiene capacidades de detección heurística (propia de la marca) que permita detectar y eliminar los virus en archivos Macro (tanto en versión ejecutable como en archivo de Microsoft Office incluyendo las nuevas versiones 2000) y además, realizar medidas probabilísticas para la detección de las posibles variantes de algún virus. Finalmente, deberá tener la capacidad de remover los macros dañados de los archivos en los cuales se detectó virus. | 2 | 3 | 3 | 3 | 3 |
| **Exploración On Access y On-Demand**<br>El software antivirus cuenta con la capacidad de exploración *on access* diferenciada en procesos de alto y bajo riesgo y deberá contar en un escaneo en demanda con la opción poder explorar los procesos en memoria. | 2 | 2 | 2 | 2 | 2 |
| **Compatibilidad con servidores de correo**<br>Compatibilidad con Microsoft Exchange Server (versiones 5.5, 2000 y 2003) y Lotus Notes / Domino Server (versiones R5 en adelante). | 1 | 2 | 2 | 2 | 2 |
| **Administración Centralizada**<br>El despliegue inicial, actualización, administración y soporte del software antivirus puede efectuarse a través de una consola de administración centralizada que cubrirá tanto los elementos locales como remotos, incluyendo estaciones de trabajo, servidores, servidores de correo electrónico, elementos en el perímetro de Internet, entre otros. Ésta consola de administración esta basada en una arquitectura jerárquica que permita un esquema *distribuido* de repositorios de instalación, que permitirán | 2 | 3 | 3 | 3 | 3 |

INTENDENCIA NACIONAL DE SISTEMAS DE INFORMACIÓN
Oficina de Investigación Tecnológica
JOSÉ ANIBAL SÁNCHEZ ZAMBRANO
EFE (e)

| | | | | | |
|---|---|---|---|---|---|
| un ahorro de ancho de banda a nivel metropolitano y nacional mientras se efectúen labores de instalación, actualización y soporte. | | | | | |
| **Instalación**<br>Las labores de instalación y despliegue a través de la consola de administración no requerirán la movilización de personal técnico hacia la estación de usuario final o equipo alguno de la red. La instalación puede hacerse de forma totalmente remota desde la consola de administración central, reconociendo a los equipos por su dirección o rango de direcciones IP, nombre, entre otros. | 2 | 3 | 3 | 3 | 3 |

| **ATRIBUTOS EXTERNOS** | **27** | **40** | | | |
|---|---|---|---|---|---|
| **Consumo de recursos**<br>La aplicación antivirus es ligera, orientada también a usuarios remotos y equipos con pocos recursos. | 2 | 3 | 3 | 2 | 3 |
| **Detección sobre el Correo Electrónico**<br>Tiene la capacidad de detectar y limpiar virus en los mensajes de correo electrónico que transiten hacia y desde el computador, en las modalidades de Microsoft Exchange (MAPI) e Internet Mail. | 2 | 3 | 3 | 3 | 3 |
| **Detección durante descarga de Archivos**<br>Capacidad de detección y limpieza de virus en los archivos que se descargan desde un servidor local o desde Internet.<br>La detección debe ser configurable sobre todos los archivos; o, configurar la detección sólo o también en archivos ejecutables, archivos con determinada extensión, archivos comprimidos, archivos con contraseña, archivos ocultos, entre otros. | 2 | 3 | 3 | 3 | 3 |
| **Detección de virus durante la navegación en Internet**<br>Capacidad de detección y limpieza de virus en los archivos que se obtienen como resultado de la navegación en Internet, y que son potencialmente dañinos, tanto para la parte física y lógica de los archivos como también para la seguridad de la información contenida en el computador del usuario. | 2 | 3 | 3 | 3 | 3 |
| **Filtro de Applets**<br>Verificación de los Controles ActiveX y Componentes o Clases JAVA. | 1 | 2 | 2 | 2 | 2 |
| **Filtro de sitios de Internet**<br>Bloqueo de direcciones IP y ubicaciones URL de Internet que contengan elementos de virus dañinos. Teniendo la capacidad de detectar automáticamente y actualizar la lista de sitios bloqueados de forma manual o automática. | 1 | 2 | 2 | 2 | 2 |
| **Instalación en cluster de servidores de correo**<br>La solución deberá estar disponible sobre servidores de correo configurados en Cluster. | 2 | 3 | 3 | 3 | 3 |
| **Detección en el perímetro de Internet**<br>Capacidades de detección y limpieza "en acceso" de virus informáticos en la puerta de acceso a Internet. Permite instalarse en computadores dedicados que contengan protocolo SMTP. Las plataformas sobre las cuales se implementara ésta solución son Windows NT, Windows | 2 | 3 | 3 | 3 | 3 |

| | | | | | |
|---|---|---|---|---|---|
| 2000, Windows Server 2003 o Sun Solaris. | | | | | |
| **Protocolos que debe soportar**<br>La protección antivirus debe estar basada sobre los protocolos HTTP, FTP y SMTP. | 3 | 3 | 3 | 3 | 3 |
| **Defensa y detección**<br>Puede detectar y limpiar virus bajo el protocolo HTTP como controles Active X y JAVA, conjuntamente con acciones de bloqueo manual o automático de direcciones IP o URL. En el protocolo FTP es posible el análisis, la detección y limpieza de archivos infectados con virus, cualquiera sea su naturaleza. | 2 | 3 | 3 | 3 | 3 |
| **Manejo del Protocolo SMTP**<br>Para el protocolo SMTP, se cuenta con la posibilidad de instalar elementos de análisis en el mismo Servidor de Correo Electrónico (como un servicio aparte) o en un computador aparte (como pasarela SMTP) para cumplir funciones de RELAY SMTP o resolución DNS para la recepción y entrega de mensajes de correo electrónico. | 2 | 3 | 3 | 3 | 3 |
| **Configuración de la detección**<br>Bloqueo de mensajes de correo electrónico no deseado, dependiendo del dominio remitente o de direcciones de correo independientes. | 2 | 3 | 3 | 3 | 3 |
| **Bloqueo de mensajes maliciosos**<br>Filtro de contenidos, que se encargará de bloquear mensajes de correo electrónico dependiendo de un texto o frase incluido en el asunto, o en el cuerpo del mensaje. Asimismo, éste filtro de contenidos se aplica a todo tipo de archivo adjunto (nombre de archivo o extensión) y a tamaños total de mensaje de correo electrónico. | 2 | 3 | 3 | 3 | 3 |
| **Administración**<br>Ofrece al administrador la capacidad de clasificar las maquinas en grupos de acuerdo con las direcciones de red. Debe incluir la comprobación de la integridad de directorio (Identificar nombres duplicados y direcciones traslapadas de IP) y debe permitir encontrar o importar automáticamente las maquinas de la red | 2 | 3 | 3 | 3 | 3 |

| | | | | | |
|---|---|---|---|---|---|
| **ATRIBUTOS DE USO** | **32** | **40** | | | |
| **Configuración de la detección en las estaciones de trabajo**<br>El software antivirus puede configurar la detección sobre todos los archivos o, configurar la detección sólo sobre archivos ejecutables, archivos con una determinada extensión, archivos comprimidos, archivos ocultos, archivos del sistema operativo en funcionamiento, o según la configuración recomendada por el archivo de actualización de firmas de virus. Así como tener la capacidad de excluir distintos tipos de carpeta de archivos en el computador con la opción de exclusión diferenciada en lectura y/o escritura. | 2 | 3 | 3 | 3 | 3 |
| **Configuración de la detección en los servidores de correo**<br>Detecta y limpia virus en archivos adjuntos a mensajes de correo electrónico. | 2 | 3 | 3 | 3 | 3 |

| | | | | | |
|---|---|---|---|---|---|
| El software antivirus tiene la capacidad de configurar la detección sobre todos los archivos adjuntos; o, configurar la detección sólo o también en archivos ejecutables, archivos con determinada extensión, archivos comprimidos, archivos con contraseña, archivos ocultos, entre otros.<br>El software debe permitir especificar las palabras y frases que no deben aparecer en la línea de asunto o el cuerpo de los mensajes de correo electrónico. | | | | | |
| **Configuración de reglas**<br>Deberá permitir la detención de brotes de infección de virus antes de que éstos sucedan, mediante la aplicación de políticas de seguridad antivirus o reglas de forma manual o automática, desde un módulo de filtro que actúe automáticamente a partir de un dato de entrada basado en: numero de infecciones en un determinado tiempo, numero de archivos adjuntos similares en un determinado tiempo. | 2 | 3 | 3 | 3 | 3 |
| **Manejo de alertas**<br>Debe permitir configurar para que informe al remitente, el destinatario y al administrador con un mensaje de alerta cuando ocurre un evento | 2 | 2 | 2 | 2 | 2 |
| **Actualización centralizada**<br>Mediante el módulo interno del software que permita mantener actualizados los productos (actualización de archivos de firma de virus y actualización de versión del software motor para todos los productos de la solución antivirus) en los clientes y servidores mediante una conexión http, ftp, recurso compartido UNC, o desde un computador previamente designado (repositorios distribuidos) y desde la consola centralizada o consola local del antivirus en forma automática, programada o cuando el usuario lo active. | 2 | 2 | 2 | 2 | 2 |
| **Actualización mediante paquetes**<br>Mediante un archivo ejecutable que permita mantener actualizados los productos (actualización de archivos de firma de virus y actualización de versión del software motor para todos los productos de la solución antivirus) en los clientes y servidores mediante la ejecución de éstos de manera local.<br>Las actualizaciones se pueden obtener directamente vía Web, e-mail o FTP. | 2 | 2 | 2 | 2 | 2 |
| **Consumo de trafico de red en la actualización**<br>El proceso de actualización de los clientes no requerirá de alto consumo de ancho de banda de los enlaces de comunicaciones, la actualización es incremental respecto a la última versión de firma de virus vigente. | 2 | 2 | 2 | 2 | 2 |
| **Notificación de actualizaciones**<br>Deberá ofrecer un software que automáticamente publique alertas de existencia de virus y ejecute la descarga de actualizaciones de archivos de firmas de virus y nuevas versiones de productos cuando estén disponibles. | 3 | 3 | 3 | 3 | 3 |
| **Actualización desatendida**<br>Se puede programar la ejecución de la instalación y actualización en los equipos cliente, servidores y otros | 2 | 3 | 3 | 2 | 3 |

INTENDENCIA NAC. DE SISTEMAS DE INFORMACION
Oficina de Investigación Tecnológica
JEFE (e)
JOSE ANIBAL SANCHEZ ZAMPERINI

| | | | | | |
|---|---|---|---|---|---|
| elementos y que ésta pueda iniciarse, administrarse y finalizar automáticamente sin intervención manual; | | | | | |
| **Almacenamiento de eventos**<br>La consola de administración puede mantener una base de datos interna o externa (SQL o similar) en la cual se almacenará en tiempo real toda la información referida a la plataforma antivirus. Esto permitirá la generación de reportes gráficos gerenciales (como gráfico de barras, lineal o de tipo pastel) o técnicos predefinidos o definidos por el usuario a través de consultas sobre la información de: | 3 | 3 | 3 | 3 | 3 |
| **Alcances del despliegue de la solución en la red**<br>Reporte de actualización de los elementos de la plataforma antivirus. Mostrando en porcentajes la distribución de las versiones del producto, motor o archivo de firma de virus. | 3 | 3 | 3 | 3 | 3 |
| **Reportes**<br>Reporte de infección en la red. Mostrando las infecciones más importantes en un determinado periodo de tiempo, las estaciones con mayor número de infecciones, etc. | 3 | 3 | 3 | 3 | 3 |
| **Distribución mediante agentes**<br>El software antivirus es totalmente compatible con sistemas de distribución y administración: Tívoli, SMS de Microsoft, entre otros. | 2 | 3 | 3 | 3 | 3 |
| **Sistema de Acciones**<br>Las acciones mínimas que el software antivirus debe tomar deberán es: Limpiar el archivo, borrar el archivo, excluir el archivo, continuar el acceso al archivo, denegar el acceso al archivo, mover el archivo, aislar el archivo y continuar el acceso al archivo. Estas acciones se pueden configurar para que el usuario escoja que tipo de acción tomar o para que el sistema ejecute ésta acción de forma automática. | 2 | 2 | 2 | 2 | 2 |
| **Modulo de Programación**<br>El software antivirus dispone de un módulo que realiza una exploración para la detección y limpieza de virus de forma programada en dispositivos locales o en la red, basado en un calendario de actividades definidas por el usuario. | 2 | 3 | 3 | 3 | 3 |

INTELIGENCIA NAC. DE SISTEMAS DE INFORMACION
Oficina de Investigación Tecnológica
JEFE (e)
JOSE ANIBAL SANCHEZ ZANABRIA

Del análisis técnico vemos que las tres herramientas cumplen con las características mínimas deseadas. Debemos tener en cuenta dos factores importantes: el primero es que desde el año 1998 SUNAT se viene utilizando el producto McAfee Active Virus Defense y que el personal de SUNAT que se encarga en dar mantenimiento y soporte a la herramienta antivirus ya cuenta con la capacitación y las habilidades para administrar esta solución, el segundo factor es que el antivirus McAfee esta considerado dentro del software estándar de la institución según la Circular 008-2006, es por este motivo que en el análisis costo beneficio solamente se considera esta herramienta.

La solución McAfee Active Virus Defense tiene además un valor agregado, esta solución ya se encuentra implementada en SUNAT, el tiempo que tomó la implementación y despliegue según el INFORME TÉCNICO No 18/7120–2006

fue de tres meses.

## 8. ANALISIS COMPARATIVO DE COSTO - BENEFICIO

Los costos asociados al producto en el corto y mediano plazo se dan a continuación:

Licenciamiento y Mantenimiento: La cotización de licenciamiento para 7000 nodos por tres años y con soporte 7x24 es de US$ 124,600.00.

Hardware: Se cuenta con el equipo necesario para la instalación de la herramienta, por lo que no es necesario realizar inversiones adicionales.

Capacitación e implementación: No es necesario tener capacitación, el personal encargado de administrar la herramienta tiene conocimiento del producto, debemos destacar que la solución McAfee Active Virus Defense ya esta implementada en SUNAT.

Para el largo plazo habría que adicionar el costo de mantenimiento que en la actualidad es de 17.80 por cada licencia.

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

## 9. CONCLUSION

Las tres soluciones analizadas cumplen con los requisitos mínimos requeridos, pero la solución McAfee Active Virus Defense se presenta como la mejor alternativa.

## 10. FIRMAS