"Año de la Integración Nacional y el Reconocimiento de Nuestra Diversidad"

Informe Técnico Previo de Evaluación de Software Antivirus

N° 01-2012/MIMP/SG/OIDS

1. Nombre del Área

Oficina de Informática y Desarrollo de Sistemas - OIDS

2. Responsable de la Evaluación

Ing. Víctor Hugo Chávez Gómez

3. Cargos

Jefe de Oficina de Informática y Desarrollo de Sistemas

4. Fecha

25 de Enero del 2012

5. Justificación

Uno de los principales riesgos para la seguridad de la información es el software malicioso, conocido comúnmente como virus informáticos. El software antivirus es producto fundamental para contrarrestar esta amenaza y actualmente el funcionamiento de computadores de usuario es inviable sin un antivirus instalado y actualizado.

El MIMP cuenta con una solución de nivel corporativo que viene funcionando desde 2008, conformada por 650 licencias del producto NOD32 y una consola de administración centralizada, que cubren los computadores de usuario, portátiles y los servidores Windows. Se requieren adquirir 650 licencias para cubrir el parque informático del MIMP.

6. Alternativas

En base a la experiencia del personal de la Oficina de Informática y Desarrollo de Sistemas, a las investigaciones realizadas a través de Internet y de la información proporcionada por los fabricantes de soluciones antivirus; se ha considerado que las siguientes soluciones constituyen las mejores alternativas para su implementación en el MIMP:

- Eset Nod32 Antivirus 5 Business
- Kaspersky Business Space Security
- McAfee Total Protection for Endpoint Advanced.

MIMP O.I.D.S. OPERACIONES

7. Análisis Comparativo Técnico

Se procedió en aplicación de la parte 3 de la Guía de Evaluación de Software:

a) Propósito de la evaluación

Determinar los atributos o características mínimas para el producto final a adquirir

b) Identificar el tipo de producto,

Solución antivirus que permitirá proporcionar la protección más rápida y mas eficiente contra todo tipo de malware como virus, spyware, adware, gusanos, troyanos, rootkits y otros ataques de Internet, manteniendo la seguridad e integridad de la información.

c) Selección de métricas

Las métricas fueron seleccionadas en base al análisis de las características de productos antivirus de nivel empresarial con administración centralizada, y los objetivos de la adquisición de la solución y a la información técnica de los productos señalados en el punto 6.- ALTERNATIVAS

En el Anexo N° 01 se presenta las características que debe cumplir la solución antivirus.

8. Análisis Comparativo de costo-beneficio:

Ver Anexo N° 02

9. Conclusiones:

Se determinaron los atributos o características técnicas mínimas para la solución antivirus, requeridas por el MIMP para la protección contra malware y virus informáticos para cubrir las estaciones de trabajo de usuarios y servidores de red.

Con la finalidad de garantizar la seguridad e integridad de los sistemas, la información, y todo recurso informático vulnerable a un ataque de software malicioso, se concluye que deben adquirirse 650 licencias corporativas de la solución antivirus Eset Nod32 Antivirus 5 Business.

10. Firmas:

MIMP O.I.D.S. OPERACIONES

ANEXO 01

Análisis Comparativo Técnico

1. Métricas

MÉTRICAS DE CALIDAD INTERNA Y EXTERNA			
Ítem	ATRIBUTOS INTERNOS Y EXTERNOS	Puntaje Máx. 84 pts	Puntaje Aprobatorio
	Funcionalidad		
1	Compatible con Sistema Operativo Windows 98, NT, Me, 2000, XP, Vista, 7	4	2
2	Compatible con Sistema Operativo Windows Server 200, 2003, 2008	4	4
3	Compatible con Sistema Operativo Linux (RHEL 4, RHEL 5, Fedora Core 8 y superiores)	4	4
4	Poseer una consola de administración centralizada, basada en protocolo TCP/IP integrada con todos los productos y componentes de protección, que permita operar remotamente y recibir información de todos los antivirus instalados en la institución.	4	4
5	Detección y eliminación automática de todo tipo de virus, troyanos, gusanos, spyware, ad-ware, keyloggers	4	2
6	Capacidad de actualización en forma automática y desatendida de todas las estaciones cliente desde un solo nodo central	4	4
7	Contar con medidas de seguridad para que el usuario no deje sin efecto políticas corporativas efectuadas en el servidor	2	2
8	Capacidad de rastrear virus en las bases de datos en formato PST	2	2
9	Capacidad de especificar exclusiones de directorios a rastrear.	2	2
10	Brindar protección para usuarios móviles. La actualización de las firmas de virus no deberá depender de estar conectado a la red institucional.	4	2
11	Capacidad de seleccionar que tipo de trafico a rastrear en el servidor (Accesos de archivos al servidor, salidas de archivos al servidor, trafico entrante y saliente).	4	2
12	Notificar los eventos de virus por diferentes medios (email, pager, etc.)	2	2
13	Mostrar reportes de los sucesos con la información Básica: Fecha, Hora, Nombre de la Maquina, nombre del archivo o componente afectado, nombre del malware	4	4
14	Capacidad de conectarse automáticamente a Internet y descargar las actualizaciones necesarias para todos los productos antivirus. La frecuencia de conexión deberá ser programable.	4	2
	Usabilidad		
15	Capacidad de seleccionar los rastreos y limpieza en tiempo real, bajo demanda, programada y remota en servidores y estaciones de trabajo.	4	2
16	Capacidad de tomar distintas acciones en caso de detección de virus (Limpiar, borrar, renombrar, eliminar, mover, o dejar pasar el archivo infectado)	4	2
17	La solución debe estar residente en el servidor y debe tener la capacidad de administrarse localmente o desde una consola central.	4	4
18	El producto debe contar un componente que nos permita scanear desde una línea de comando a cualquier archivo entrante.	4	2
19	La consola debe estar estructurada según un agrupamiento lógico	4	4

MIMP V.B. OPERACIONES

MÉTRICAS DE CALIDAD INTERNA Y EXTERNA			
Ítem	ATRIBUTOS INTERNOS Y EXTERNOS	Puntaje Máx. 84 pts	Puntaje Aprobatorio
	de funciones y tareas, con capacidad para configurar parámetros, programar ejecución de tareas y ejecutar bajo comando tareas en las estaciones cliente.		
20	Capacidad para actualizarse de manera alternativa utilizando un recurso compartido, CD ROM o disquetes, en caso de no contar con una conexión a Internet y desplegar la actualización a los productos antivirus que controla	4	4
21	Programar la descarga de actualizaciones de firmas de virus y de motores de búsqueda, en un repositorio centralizado para su uso por todos los módulos de la solución	4	4
22	Tiempo en aprender los usuarios el manejo del software antivirus para tomar acciones ante un evento y/o una necesidad (usuarios familiarizados con la interfaz grafica)	4	2
	Eficiencia		
23	Funcionar sin impactar significativamente el funcionamiento y performance de los equipos ni durante la exploración ni en la operación en tiempo real.	4	2
	TOTAL	**84**	**64**

MÉTRICAS DE CALIDAD DE USO			
Ítem	ATRIBUTOS DE USO	Puntaje Máx. 16 pts	Puntaje Aprobatorio
	Eficacia		
24	Capacidad de producto de software para permitir a los usuarios lograr las metas especificadas.	4	4
	Productividad		
25	Capacidad del producto de software para permitir a los usuarios emplear cantidades apropiadas de recursos en relación a la eficacia lograda en un contexto especificado de uso.	4	2
	Satisfacción		
26	Capacidad del producto de software para satisfacer a los usuarios en un contexto especificado de uso.	4	2
	Seguridad		
27	La capacidad del producto de software para lograr niveles aceptables de riesgo a la institución, software, propiedad o entorno.	4	4
	TOTAL	**16**	**12**

2. Comparación de Productos

MÉTRICAS DE CALIDAD INTERNA Y EXTERNA						
Ítem	ATRIBUTOS INTERNOS Y EXTERNOS	Punt. Máx.	Punt. Aprob	Eset Nod32 Antivirus 5 Business	Kaspersky Business Space Security	McAfee Total Protection
	Funcionalidad					
1	Compatible con Sistema Operativo Windows 98, NT, Me, 2000, XP, Vista, 7	4	2	4	4	2
2	Compatible con Sistema Operativo Windows Server 200, 2003, 2008	4	4	4	4	4
3	Compatible con Sistema Operativo Linux (RHEL 4, RHEL 5, Fedora Core 8 y superiores)	4	4	4	4	4
4	Poseer una consola de administración centralizada, basada en protocolo TCP/IP integrada con todos los productos y componentes de protección, que permita operar remotamente y recibir información de todos los antivirus instalados en la institución.	4	4	4	4	4
5	Detección y eliminación automática de todo tipo de virus, troyanos, gusanos, spyware, ad-ware, keyloggers.	4	2	4	4	4
6	Capacidad de actualización en forma automática y desatendida de todas las estaciones cliente desde un solo nodo central.	4	4	4	4	4
7	Contar con medidas de seguridad para que el usuario no deje sin efecto políticas corporativas efectuadas en el servidor.	2	2	2	2	2
8	Capacidad de rastrear virus en las bases de datos en formato PST.	2	2	2	2	2
9	Capacidad de especificar exclusiones de directorios a rastrear.	2	2	2	2	2
10	Brindar protección para usuarios móviles. La actualización de las firmas de virus no deberá depender de estar conectado a la red institucional.	4	2	4	4	4
11	Capacidad de seleccionar que tipo de trafico a rastrear en el servidor (Accesos de archivos al servidor, salidas de archivos al servidor, trafico entrante y saliente).	4	2	4	4	4
12	Notificar los eventos de virus por diferentes medios (email, pager, etc.)	2	2	2	2	2
13	Mostrar reportes de los sucesos con la información Básica: Fecha, Hora, Nombre de la Maquina, nombre del archivo o componente afectado, nombre del malware.	4	4	4	4	4
14	Capacidad de conectarse automáticamente a Internet y descargar las actualizaciones necesarias para todos los productos antivirus. La frecuencia de conexión deberá ser programable.	4	2	4	4	4
	Usabilidad					
15	Capacidad de seleccionar los rastreos y limpieza en tiempo real, bajo demanda, programada y remota en servidores y estaciones de trabajo.	4	2	4	4	4
16	Capacidad de tomar distintas acciones en caso de detección de virus (Limpiar, borrar, renombrar, eliminar, mover, o dejar pasar el archivo infectado).	4	2	4	4	4

MÉTRICAS DE CALIDAD INTERNA Y EXTERNA						
Ítem	ATRIBUTOS INTERNOS Y EXTERNOS	Punt Máx.	Punt. Aprob	Eset Nod32 Antivirus 5 Business	Kaspersky Business Space Security	McAfee Total Protection
17	La solución debe estar residente en el servidor y debe tener la capacidad de administrarse localmente o desde una consola central.	4	4	4	4	4
18	El producto debe contar un componente que nos permita escanear desde una línea de comando a cualquier archivo entrante.	4	2	2	2	0
19	La consola debe estar estructurada según un agrupamiento lógico de funciones y tareas, con capacidad para configurar parámetros, programar ejecución de tareas y ejecutar bajo comando tareas en las estaciones cliente.	4	4	4	4	4
20	Capacidad para actualizarse de manera alternativa utilizando un recurso compartido, CD ROM o disquetes, en caso de no contar con una conexión a Internet y desplegar la actualización a los productos antivirus que controla	4	4	4	4	4
21	Programar la descarga de actualizaciones de firmas de virus y de motores de búsqueda, en un repositorio centralizado para su uso por todos los módulos de la solución	4	4	4	4	4
22	Tiempo en aprender los usuarios el manejo del software antivirus para tomar acciones ante un evento y/o una necesidad (usuarios familiarizados con la interfaz grafica)	4	2	4	2	2
	Eficiencia					
23	Funcionar sin impactar significativamente el funcionamiento y performance de los equipos ni durante la exploración ni en la operación en tiempo real.	4	2	4	2	2
	TOTAL	**84**	**64**	**82**	**78**	**74**

MIMP O.I.D.S. OPERACIONES

MÉTRICAS DE CALIDAD DE USO						
Ítem	ATRIBUTOS DE USO	Punt. Máx.	Punt. Aprob	Eset Nod32 Antivirus 5 Business	Kaspersky Business Space Security	McAfee Total Protection
	Eficacia					
24	Capacidad de producto de software para permitir a los usuarios lograr las metas especificadas.	4	4	4	4	4
	Productividad					
25	Capacidad del producto de software para permitir a los usuarios emplear cantidades apropiadas de recursos en relación a la eficacia lograda en un contexto especificado de uso.	4	2	4	2	2
	Satisfacción					
26	Capacidad del producto de software para satisfacer a los usuarios en un contexto especificado de uso.	4	2	4	2	2
	Seguridad					
27	La capacidad del producto de software para lograr niveles aceptables de riesgo a la institución, software, propiedad o entorno.	4	4	4	4	4
	TOTAL	**16**	**12**	**16**	**12**	**12**

RESUMEN EVALUACIÓN TÉCNICA			
	Eset Nod32 Antivirus 5 Business	**Kaspersky Business Space Security**	**McAfee Total Protection**
Total Métricas de Calidad del Producto	82	78	74
Total Métricas de Calidad de Uso	16	12	12
TOTAL	**98**	**90**	**86**

Podemos observar que en la evaluación Técnica el mayor puntaje obtenido es el Eset Nod32 Antivirus 5 Business con 98 puntos, seguido de Kaspersky Business Space Security con 90 puntos y McAfee Total Protection con 86 puntos.

ANEXO 02
Análisis Comparativo Costo – Beneficio

Para efectuar el análisis de Costo Beneficio se tiene en cuenta lo expresado en los siguientes cuadros:

VALORACIÓN DE LA CALIDAD DE USO:

$$\textbf{TOTAL} = \frac{\text{METRICA DE CALIDAD DE USO + VALORACION PRODUCTO}}{2}$$

Resultado de la Valoración de Producto:

Valoración	Eset Nod32 Antivirus 5 Business	Kaspersky Business Space Security	McAfee Total Protection
Calidad de Producto	82	78	74
Calidad de uso	16	12	12
Valoración de la Calidad de uso	**49**	**45**	**43**

VALORACION DEL COSTO DE LICENCIAMIENTO:

Costo	Puntaje
Costo Alto	1
Costo Medio	2
Costo Bajo	3

Valoración de referencia:

Producto	Precio Estimado por Licencia (*)	Precio Estimado por 650 Licencias (*)	Valoración
Kaspersky Business Space Security	S/. 97.87	S/. 63,615.50	**1**
McAfee Total Protection	S/. 53.34	S/. 34,671.00	**2**
Eset Nod32 Antivirus 5 Business	S/. 49.18	S/. 31,967.00	**3**

(*) Expresado en Nuevo Soles (S/.), Incluido I.G.V.
Tipo de cambio s/.2.8 = $1
Fuente: Cotizaciónes y Pagina Web

Se puede observar que **Eset Nod32 Antivirus 5 Business** es el menos costoso por ende se asigna una valoración de tres (3), seguido por su competidor **McAfee Total Protection** donde se asigna una valoración de dos (2) y finalmente **Kaspersky Business Space Security** con una valoración de uno (1).

MIMP O.I.O.S. OPERACIONES

VALORACIÓN DEL COSTO DE HARDWARE NECESARIO PARA SU FUNCIONAMIENTO

El costo del hardware necesario para el funcionamiento de la solución antivirus es cero soles (s/.0.0) debido que no necesita de hardware adicional para la implementación del software ya que se cuenta con la infraestructura (hardware) necesaria para la administración y funcionamiento del total de las licencias para cualquiera de los tres productos. Por ende no se valoriza este concepto o es nulo.

VALORACION DEL COSTO DE SOPORTE Y MANTENIMIENTO EXTERNO

El costo del soporte y mantenimiento externo es nulo ya que esta incluido en el costo de adquisición de las licencias en los tres productos, haciendo un costo cero (S/.0.0) en este concepto.

VALORACION DEL COSTO DE PERSONAL Y MANTENIMIENTO INTERNO

No será necesario la contratación de nuevo personal para administrar la consola de antivirus ni para el mantenimiento interno del mismo, debido que la institución cuenta con personal designada para esta función. Se concluye que el costo del personal y mantenimiento interno es un costo nulo o cero soles (s/.0.00).

VALORACION DEL COSTO DE CAPACITACION

Los tres productos ofrecen capacitación en la administración, configuración y ejecución de sus respectivos productos. El costo de dicha capacitación es nulo o cero soles (S/.0.00) ya que también esta incluido dentro del costo de las licencias en los tres productos.

VALORACIÓN DEL COSTO TOTAL

COSTOS	Eset Nod32 Antivirus 5 Business	Kaspersky Business Space Security	McAfee Total Protection
Valoración del costo de licenciamiento.	3	1	2
Valoración del costo de hardware necesario para su funcionamiento	-	-	-
Valoración del costo de soporte y Mantenimiento.	-	-	-
Valoración del costo de personal y Mantenimiento interno.	-	-	-
Valoración del costo de capacitación.	-	-	-
VALORACIÓN DEL COSTO TOTAL	**3**	**1**	**2**

NOTA: No se le da valoración a los cuatro últimos costos, debido que en los tres productos están incluidos dentro del costo de adquisición de las licencias en similares características.

IMPACTO EN EL CAMBIO DE PLATAFORMA

Cabe resaltar que los usuarios de la institución (MIMP) se encuentran familiarizados con la interfaz grafica del antivirus (NOD32), además no es necesario reinstalar el producto en las estaciones de trabajo, ya se encuentran configurado en ellas, por consiguiente solo se actualizaría las licencias evitando montar un despliegue de recursos para la reinstalación de un nuevo antivirus, a diferencia de Karspesky o McAffe que se tendría que instalar las 650 licencias en toda la institución además de generar malestar a los usuarios.

VALORACION TOTAL

$$\textbf{TOTAL} = \frac{\text{METRICA DE CALIDAD DE USO + VALORACION DEL PRECIO}}{2}$$

Valoración final:

Valoración	Eset Nod32 Antivirus 5 Business	Kaspersky Business Space Security	McAfee Total Protection
Valoración de la Calidad de Uso	49	45	43
Valoración del Costo Total	3	1	2
VALORACIÓN TOTAL	**26**	**23**	**22.5**

Se observa en la tabla con la mayor valoración obtenida es la solución Eset Nod32 Antivirus 5 Business con una valoración total de 26, seguido por Kaspersky Business Space Security con 23 y McAfee Total Protection con 22.5 de valoración.

Se selecciona la Alternativa **01**: **Eset Nod32 Antivirus 5 Business**
Por ser uno de los mas económicos y demostró ser mas eficiente para las necesidades de la institución.

Por consiguiente al adquirir la solución Eset Nod32 Antivirus 5 Business con las características técnicas requeridas, permitirá proporcionar la protección más rápida, más eficiente y una de las más económicas del mercado que nos permitirá mantener la seguridad e integridad de la información contra todo tipo de malware.

MIMP O.I.D.S. OPERACIONES