

**INFORME TÉCNICO PREVIO EVALUACIÓN DE SOFTWARE DE ANTIVIRUS**

N° 01-2011-ANA-OSNIRH

1. Nombre del Área.

Oficina del Sistema Nacional de Información de Recursos Hídricos

2. Responsable de la Evaluación

Ing. Néstor Dino Giuseppe Bermúdez Corzano

Tec. Pablo Demetrio Carrión Méndez

3. Cargos

Administrador de Red

Especialista en Soporte Técnico

4. Fecha

05 de Octubre del 2011

5. Justificación.

Uno de los principales riesgos de la seguridad de la información son los virus informáticos (virus, gusanos, troyanos, spyware, adware, phishing y cualquier otro tipo de código malicioso), por lo que el software antivirus es un producto fundamental para controlar todos los datos entrantes y salientes, incluyendo correo electrónico, tráfico de correo y todas las interacciones de red, asimismo garantizar la protección de estaciones de trabajo y dispositivos móviles, garantizando un acceso seguro y rápido a los recursos de la red e Internet, así como comunicaciones seguras por correo electrónico; mitigando cualquier amenaza; de esta manera asegurar un adecuado funcionamiento del equipo de cómputo.

La Autoridad Nacional del Agua, cuenta con una solución de software antivirus de nivel corporativo, que viene operando desde del 2009, siendo esta en un número de 1200 licencias del producto Kaspersky Total Space Security con una consola de administración centralizada que cubre las computadoras de los usuarios, los equipos portátiles y los servidores Windows.

Debido a que las licencia caducan en el mes de Diciembre, es necesario adquirir 1200 licencias adicionales de solución antivirus.

6. Alternativas.

En base a la experiencia del personal de la Oficina del Sistema Nacional de Información de Recursos Hídricos, las investigaciones realizadas a través de Internet y la información proporcionada por los fabricantes se ha considerado las siguientes soluciones de software antivirus como las mejores alternativas para la implementación en la Autoridad Nacional del Agua:

- Kaspersky Total Space Security.
- Eset NOD 32 Antivirus 4 Business.
- BitDefender.





7. Análisis Comparativo Técnico

El informe se ha realizado utilizando los parámetros establecidos en la RM 139-2004-PCM "Guía Técnica sobre Evaluación de Software en la Administración Pública".

a) Objetivo

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

b) Identificar el tipo de producto.

Solución Antivirus que permitirá proporcionar la protección más rápida y más 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) Consideraciones Previas

El producto a evaluar es un software de antivirus que sea capaz de trabajar en un entorno de red con estaciones Pentium IV, Windows XP Professional SP3 - 32 Bits, Windows Vista - 64 Bits, Windows 7 en 32 Bits y 64 Bits y con servidores cuyos Sistemas Operativos son Windows Server 2003, 2008 y Sistema Operativo Linux (RHEL 4, RHEL 5, Fedora Core 8)

d) 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 la Autoridad Nacional del Agua para la protección contra malware y virus informático 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, concluye las tres soluciones de software antivirus tienen el mismo puntaje.

10. Firmas:

Ing. Néstor Dino Giuseppe Bermúdez Corzano
Administrador de Red
Autoridad Nacional del Agua

Tec. Pablo Demetrio Carrión Méndez
Especialista en Soporte Técnico
Autoridad Nacional del Agua



ANEXO 01

Análisis Comparativo Técnico

1.- Métricas:

METRICAS DE CALIDAD INTERNA Y EXTERNA			
Item	Atributos internos y Externos	Puntaje Max. 84 pts.	Puntaje Aprobatorio 64 pts.
	Funcionalidad		
1	Compatibilidad con Sistema Operativo 2000, XP, Vista, 7 en 32 Bits y 64 Bits.	4	2
2	Compatible con Sistema Operativo Server 2003 y 2008	4	4
3	Compatible con Sistema Operativo Linux (RHEL 4, RHEL 5, Fedora, Core 8 y superiores)	4	4
4	Contar con 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 los equipo de 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 todos las estaciones cliente desde un solo nodo central.	4	4
7	Contar con medidas de seguridad para que el usuario cliente no deje modifique políticas corporativas efectuadas desde el servidor.	2	2
8	Capacidad de rastrear virus en las bases de datos en forma PST.	2	2
9	Capacidad de especificar exclusiones de direcciones a rastrear.	2	2
10	Brindar protección para usuarios móviles. La actualización de las firmas de virus no deberá depender de estar conectado al servicio de Internet de la red institucional.	4	2
11	Capacidad de seleccionar que tipo de tráfico a rastrear en el servidor (Accesos de archivos al servidor, salidas de archivos al servidor, tráfico entrante y saliente).	4	2





METRICAS DE CALIDAD INTERNA Y EXTERNA

Item	Atributos internos y Externos	Puntaje Max. 84 pts.	Puntaje Aprobatorio 64 pts.
12	Notificar los eventos de virus por diferentes medios (e-mail, pager, etc.).	2	2
13	Mostrar reportes de los sucesos con la información básica: fecha, hora, nombre de la pc, nombre de archivo o componente infectado, nombre del malware.	4	4
14	Capacidad de conectarse automáticamente a Internet y descargar las actualizaciones necesarias para toda la solución antivirus; asimismo la frecuencia de conexión debe 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 acciones en caso de detección de virus (desinfectar, 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 la 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 de funciones y tareas, con capacidad para configurar parámetros, programar ejecución de tareas y ejecutar bajo comando tareas en las estaciones cliente.	4	4
20	Capacidad para actualizarse de manera alternativa utilizando un recurso compartido, CD-ROM o cualquier otro medio de almacenamiento, en caso de no contar con el servicio de Internet.	4	4
21	Que permita programar la descarga de actualizaciones de firmas de virus y de motores de búsqueda, en un repositorio centralizado para uso de todos los módulos de la solución.	4	4
22	Tiempo en capacitar al usuario en el manejo y uso del software antivirus, para tomar acciones ante un evento y/o	4	2





PERU

Ministerio de
AgriculturaAutoridad Nacional
del AguaOficina del Sistema Nacional de
Información de los Recursos Hídricos

METRICAS DE CALIDAD INTERNA Y EXTERNA			
Item	Atributos internos y Externos	Puntaje Max. 84 pts.	Puntaje Aprobatorio 64 pts.
	necesidad (usuarios familiarizados con la interfaz gráfico).		
	Eficiencia		
23	Funcionar sin afectar significamente el rendimiento y performance del equipo ni durante la exploración ni en la operación en tiempo real.	4	2
	TOTAL	84	64

METRICAS DE CALIDAD DE USO			
Item	Atributos de Uso	Puntaje Max. 16 pts.	Puntaje Aprobatorio 12 pts.
	Eficacia		
24	Capacidad del producto para que los usuario logren 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	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.

METRICAS DE CALIDAD INTERNA Y EXTERNA						
Item	Atributos internos y Externos	Puntaje Max. 84 pts.	Puntaje Aprob. 64 pts.	Eset Nod32 Antivirus 4 Business	Kaspersky Total Space Security	Bitdefender
	Funcionalidad					
1	Compatibilidad con Sistema Operativo 2000, XP, Vista, 7 en 32 Bits y 64 Bits.	4	2	4	4	4
2	Compatible con Sistema Operativo Server 2003 y 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	Contar con 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 los equipo de 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 todos las estaciones cliente desde un solo nodo central.	4	4	4	4	4
7	Contar con medidas de seguridad para que el usuario cliente no deje modifique políticas corporativas efectuadas desde el servidor.	2	2	2	2	2
8	Capacidad de rastrear virus en las bases de datos en forma PST.	2	2	2	2	2
9	Capacidad de especificar exclusiones de direcciones 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	4	2	4	4	4





PERÚ

Ministerio de
AgriculturaAutoridad Nacional
del AguaOficina del Sistema Nacional de
Información de los Recursos Hídricos

METRICAS DE CALIDAD INTERNA Y EXTERNA

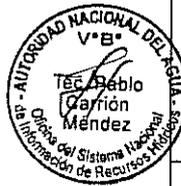
Item	Atributos internos y Externos	Puntaje Max. 84 pts.	Puntaje Aprob. 64 pts.	Eset Nod32 Antivirus 4 Business	Kaspersky Total Space Security	Bitdefender
	conectado al servicio de Internet de la red institucional.					
11	Capacidad de seleccionar que tipo de tráfico a rastrear en el servidor (Accesos de archivos al servidor, salidas de archivos al servidor, tráfico entrante y saliente).	4	2	4	4	4
12	Notificar los eventos de virus por diferentes medios (e-mail, pager, etc.).	2	2	2	2	2
13	Mostrar reportes de los sucesos con la información básica: fecha, hora, nombre de la pc, nombre de archivo o componente infectado, nombre del malware.	4	4	4	4	4
14	Capacidad de conectarse automáticamente a Internet y descargar las actualizaciones necesarias para toda la solución antivirus; asimismo la frecuencia de conexión debe 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 acciones en caso de detección de virus (desinfectar, renombrar, eliminar, mover o dejar pasar el archivo infectado).	4	2	4	4	4
17	La solución debe estar residente en el servidor y debe tener la capacidad de administrarse localmente o desde la consola central.	4	4	4	4	4
18	El producto debe contar un componente que nos permita scanear desde una línea de comando a cualquier archivo	4	2	2	2	2





METRICAS DE CALIDAD INTERNA Y EXTERNA

Item	Atributos internos y Externos	Puntaje Max. 84 pts.	Puntaje Aprob. 64 pts.	Eset Nod32 Antivirus 4 Business	Kaspersky Total Space Security	Bitdefender
	entrante.					
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 cualquier otro medio de almacenamiento, en caso de no contar con el servicio de Internet.	4	4	4	4	4
21	Que permita programar la descarga de actualizaciones de firmas de virus y de motores de búsqueda, en un repositorio centralizado para uso de todos los módulos de la solución.	4	4	4	4	4
22	Tiempo en capacitar al usuario en el manejo y uso del software antivirus, para tomar acciones ante un evento y/o necesidad (usuarios familiarizados con la interfaz gráfico).	4	2	2	4	2
	Eficiencia					
23	Funcionar sin afectar significativamente el rendimiento y performance del equipo ni durante la exploración ni en la operación en tiempo real.	4	2	4	4	4
	TOTAL	84	64	80	82	80





METRICAS DE CALIDAD DE USO						
Item	Atributos de Uso	Puntaje Max. 16 pts.	Puntaje Aprob. 12 pts.	Eset Nod32 Antivirus 4 Business	Kaspersky Open Space Security	Bitdefender
	Eficacia					
24	Capacidad del producto para que los usuario logren 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	4	4
	Satisfacción					
26	Capacidad del producto de software para satisfacer a los usuarios en un contexto especificado de uso.	4	2	2	4	4
	Seguridad					
27	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	14	16	16



RESUMEN DE EVALUACION TÉCNICA			
Métricas	Eset Nod32 Antivirus 4 Business	Kaspersky Open Space Security	Bitdefender
Total de Métricas de Calidad del Producto	80	82	80
Total de Métricas de Calidad de Uso	14	16	16
TOTAL	94	98	96

Podemos observar que en la Evaluación Técnica el mayor puntaje obtenido es el Kaspersky Total Space Security, con 98 puntos, seguido del software Bitdefender con 96 puntos y Eset Nod32 Antivirus 4 Business con 94 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:			
TOTAL = $\frac{\text{METRICA DE CALIDAD DE USO} + \text{VALORACIÓN PRODUCTO}}{2}$			
VALORACION	Eset Nod32 Antivirus 4 Business	Kaspersky Total Space Security	Bitdefender
Total Métricas de Calidad del Producto	80	82	80
Total Métricas de Calidad de Uso	14	16	16
RESULTADO VALORACION DEL PRODUCTO	47	49	48

VALORACION DEL COSTO DE LICENCIAMIENTO:



Costo	Puntaje
Alto Costo	1
Costo Medio	2
Costo Bajo	3

Valoración de referencia:



Producto	Precio Estimado por Licencia (*)	Precio estimado por 300 Licencias (*)	Valoración
Eset Nod32 Antivirus 4 Business	S/. 46.11	S/. 55,332.00	3
Kaspersky Total Space Security	S/. 48.35	S/. 58,020.00	1
Bitdefender	S/. 46.88	S/. 56,256.00	2

(*) Precios incluyen IGV.

Se puede observar que el Eset Nod 32 Antivirus 4 Business es el menos costoso por ende se le asigna una valoración de tres (3).



PERÚ

Ministerio de
Agricultura

Autoridad Nacional
del Agua

Oficina del Sistema Nacional de
Información de los Recursos Hídricos

VALORACIÓN TOTAL

TOTAL = <u>METRICA DE CALIDAD DE USO + VALORACIÓN DEL COSTO TOTAL</u>			
2			
VALORACION	<i>Eset Nod32 Antivirus 4 Business</i>	<i>Kaspersky Total Space Security</i>	Bitdefender
VAOLORACIÓN DE LA CALIDAD DE USO	47	49	48
VALORACIÓN DEL COSTO TOTAL	3	1	2
VALORACION TOTAL	25	25	25



Se observa que los tres productos obtienen 25 puntos.





VALORACION DEL COSTO DE HARDWARE NECESARIO PARA SU FUNCIONAMIENTO

El costo del hardware para el funcionamiento de la solución antivirus es Cero Nuevos Soles (S/. 0.00), porque no se necesita hardware adicional para la implementación de la solución antivirus. La institución cuenta con todo lo necesario.

VALORACION DEL COSTO DE SOPORTE Y MANTENIMIENTO EXTERNO.

Esta valoración no es considerada porque está incluido en el costo de adquisición de las nuevas licencias en los 3 productos.

VALORACIÓN DEL COSTO DE PERSONAL Y MANTENIMIENTO INTERNO

No será necesaria la contratación de un personal adicional, ya que la institución cuenta con el personal designado para esta función.

VALORACIÓN DEL COSTO DE CAPACITACIÓN.

Los 3 productos han contemplado dentro de sus cotizaciones la capacitación en la administración, configuración y ejecución de sus respectivos productos; por lo que el costo por capacitación sería S/. 0.00 nuevos soles.

VALORACION DEL COSTO TOTAL

COSTOS	Eset Nod32 Antivirus 4 Business	Kaspersky Total Space Security	Bitdefender
VALORACION DEL COSTO DE LICENCIAMIENTO	3	1	2
VALORACION DEL COSTO DE HARDWARE NECESARIO PARA SU FUNCIONAMIENTO	0	0	0
VALORACION DEL COSTO DE SOPORTE Y MANTENIMIENTO EXTERNO.	0	0	0
VALORACIÓN DEL COSTO DE PERSONAL Y MANTENIMIENTO INTERNO	0	0	0
VALORACIÓN DEL COSTO DE CAPACITACIÓN.	0	0	0
VALORACION COSTO TOTAL	3	1	2

IMPACTO EN EL CAMBIO DE PLATAFORMA

Cabe resaltar que los usuarios de la institución (ANA) se encuentran familiarizados con la interfaz gráfica del antivirus Kaspersky Total Space Security; además no es necesario reinstalar el producto en las estaciones de trabajo; ya que se encuentran configurados en ellas; por consiguiente sólo se actualizaría el número y tipo de licencias evitando montar un despliegue de recursos para la reinstalación de un nuevo antivirus, a diferencia de Eset Nod32 Antivirus 4 Business o Bitdefender que se tendría que reinstalar la totalidad de las licencias en toda la institución, además de generar malestar a los usuarios.

