HOSPITAL VICTOR LARCO HERRERA

INFORME PREVIO DE EVALUACION DE SOFTWARE ANTIVIRUS

1. NOMBRE DEL AREA:

Equipo de Informática.

2. RESPONSABLES DE LA EVALUACION:

Andrés Emerson Quiroz López

3. CARGO(S):

Soporte técnico

4. FECHA

22 de Julio del 2008

5. JUSTIFICACION

Establecer los atributos o características mínimas para software antivirus que serán utilizadas en la adquisición de licencias.

6. ALTERNATIVAS

Se analizarán los siguientes productos antivirus

- McAfee Antivirus
- ESET NOD32 Antivirus
- Kaspersky Antivirus

7. ANALISIS COMPARATIVO TECNICO

Se realizó aplicando la parte 3 de la Guía de Evaluación de Software:

a. **Propósito de evaluación**
   Determinar los atributos o características mínimas para el producto final del software antivirus

b. **Identificar el tipo de producto**

MINISTERIO DE SALUD
HOSPITAL "VICTOR LARCO HERRERA"
Sr. EDGAR TUESTA RAMOS
Director de la Oficina de Estadística e Informática

MINISTERIO DE SALUD
HOSPITAL "VICTOR LARCO HERRERA"
Sr. EDGAR TUESTA RAMOS
Director de la Oficina de Estadística e Informática

ANTIVIRUS CORPORATIVO PARA ESTACIONES DE TRABAJO Y SERVIDORES

c. Especificación del Modelo de Calidad

Se aplicará el Modelo de calidad de Software descrito en la Parte I de la Guía de Evaluación de Software aprobado por Resolución Ministerial N° 139-2004-PCM

d. Selección de Métricas

Las métricas fueron seleccionadas en base al análisis de la información técnica de los productos antivirus señalados en el punto "6. ALTERNATIVAS ", como son las características del Producto y Requerimientos de Instalación y que fueron obtenidas de las siguientes empresas proveedoras de software:

- Cosapi Data S.A.C. – distribuidor de McAfee Antivirus.
- OpenLatam S.A.C. – distribuidor de Eset NOD32 Antivirus.
- Softland Peru S.A.C. – distribuidor de Karpesky Antivirus.

Del análisis realizado se ha determinado las siguientes características técnicas mínimas:

ATRIBUTOS INTERNOS		
1	Sistemas Operativos Estaciones de Trabajo	Microsoft Windows 2000 PROF, XP PROFESIONAL, WINDOWS VISTA, LINUX
2	Sistemas Operativos Servidores de Red	Microsoft 2000 Server, Microsoft Server 2003, y Linux.
3	Actualizaciones	Manuales y automáticas (programadas) del fichero de firmas de virus y del motor de búsqueda en los servidores y estaciones de trabajo desde Internet. Debe brindar la creación de repositorios distribuidos programados.
4	Compatibilidad	Carta del fabricante del software antivirus indicando la total compatibilidad con los sistemas operativos anteriormente mencionados
5	Instalación	La instalación del software a la computadora de los usuarios debe de ser directamente desde la consola de administración, además de la posibilidad de instalación mediante CD o recurso UNC.
ATRIBUTOS EXTERNOS		
6	Administración	Capacidad de despliegue, instalación, actualización y monitoreo de software antivirus a través de la consola de administración
		La administración centralizada no debe requerir un servidor dedicado.
		Configuración para formar grupos de equipos y

MINISTERIO DE SALUD
HOSPITAL "VICTOR LARCO HERRERA"

Sr. EDGAR PUESTA RAMOS
Director de la Oficina de Estadistica é Informatica

	Defensa en los servidores de Red	9
	Escaneo	9
ATRIBUTOS DE USO		
	Alertas y Reportes	9
	Facilidad de Uso	6
	Soporte técnico a usuarios	7
	Eficacia	8
	Productividad	8
PUNTAJE TOTAL		**100**

EVALUACION TECNICA DE MCAFEE ANTIVIRUS

ATRIBUTOS INTERNOS		
	Sistemas Operativos, Estaciones de Trabajo	4
	Sistemas Operativos Servidores de Red	5
	Actualizaciones	8
	Compatibilidad	6
	Instalación	3
ATRIBUTOS EXTERNOS		
	Administración	6
	Defensa contra: Virus , Virus Troyanos, Macro Virus, Virus Gusano, Virus en archivos comprimidos	8
	Defensa en los servidores de Red	9
	Escaneo	9
ATRIBUTOS DE USO		
	Alertas y Reportes	8
	Facilidad de Uso	6
	Soporte técnico a usuarios	7
	Eficacia	8
	Productividad	8
PUNTAJE TOTAL		96

EVALUACION TECNICA DE ESET NOD32 ANTIVIRUS

ATRIBUTOS INTERNOS		
	Sistemas Operativos, Estaciones de Trabajo	5
	Sistemas Operativos Servidores de Red	5
	Actualizaciones	8
	Compatibilidad	8
	Instalación	3
ATRIBUTOS EXTERNOS		
	Administración	7

MINISTERIO DE SALUD
HOSPITAL "VICTOR LARCO HERRERA"

Sr. EDGAR TUESTA RAMOS
Director de la Oficina de Estadística e Informática

	Defensa contra: Virus , Virus Troyanos, Macro Virus, Virus Gusano, Virus en archivos comprimidos	8
	Defensa en los servidores de Red	9
	Escaneo	9
ATRIBUTOS DE USO		
	Alertas y Reportes	9
	Facilidad de Uso	6
	Soporte técnico a usuarios	7
	Eficacia	8
	Productividad	8
	PUNTAJE TOTAL	100

EVALUACION TECNICA DE KASPERSKY ANTIVIRUS

ATRIBUTOS INTERNOS		
	Sistemas Operativos, Estaciones de Trabajo	4
	Sistemas Operativos Servidores de Red	5
	Actualizaciones	8
	Compatibilidad	7
	Instalación	3
ATRIBUTOS EXTERNOS		
	Administración	6
	Defensa contra: Virus , Virus Troyanos, Macro Virus, Virus Gusano, Virus en archivos comprimidos	8
	Defensa en los servidores de Red	9
	Escaneo	9
ATRIBUTOS DE USO		
	Alertas y Reportes	7
	Facilidad de Uso	6
	Soporte técnico a usuarios	7
	Eficacia	8
	Productividad	8
	PUNTAJE TOTAL	96

De esta evaluación se estableció las siguientes características mínimas del software antivirus.

MINISTERIO DE SALUD
HOSPITAL "VICTOR LARCO HERRERA"

Sr. EDGAR TUESTA RAMOS
Director de la Oficina de Estadistica é Informatica

ESPECIFICACIONES TÉCNICAS DE LICENCIA CORPORATIVA DE ANTIVIRUS

REQUERIMIENTOS TÉCNICOS MÍNIMOS

Generalidades

LA ENTIDAD, desea adquirir una solución de software que proteja la red así como los servicios de Correo, Internet y Aplicaciones de programas tales como los virus, spyware, gusanos, troyanos, spam y todo tipo de programa malicioso.

La solución deberá identificar las amenazas o debilidades de la infraestructura de red y deberá tomar acciones, previniendo incidentes antes de que las amenazas informáticas impacten negativamente en los recursos (activos) de la red.

LA ENTIDAD requiere comprar la licencia corporativa Antivirus para 140 equipos. software para la protección de las estaciones de trabajo, 140 usuarios independiente, los servidores de aplicaciones y/o datos, la consola de administración centralizada y el servidor de correos Linux.

Para todos los productos se requiere las últimas versiones liberadas por los fabricantes. No se aceptarán versiones beta, en etapas de desarrollo tempranas o **"versiones anteriores"**.

La solución de software ofertada deberá de tener una licencia de suscripción por un año con mantenimiento de software, incluye bases de datos de firmas, updates y upgrades de la solución ofertada.

La solución ofertada deberá de ser una solución totalmente basada en software y no dependiente de ningún hardware propietario ("appliance").

El postor deberá adjuntar folletos o direcciones de páginas de web del fabricante donde indique expresamente que la última versión liberada soporta las plataformas de sistemas operativos solicitados en la presente bases. Asimismo deberá sustentar el cumplimiento de estas características técnicas con una Carta del Fabricante.

Especificaciones Técnicas Mínimas

Estaciones de Trabajo, Servidores y Consola de Administración

Estaciones de Trabajo

El antivirus ofertado deberá de soportar los sistemas operativos MS Windows XP PROFESSIONA, Windows VISTA, MS Windows 2000 Professional.

MINISTERIO DE SALUD
HOSPITAL "VICTOR LARCO HERRERA"
Sr. EDGAR TUESTA RAMOS
Director de la Oficina de Estadística é Informatica

El antivirus ofertado deberá de detectar virus, troyanos, macro virus, gusano y malware en todos los archivos, o tipos de archivos, residentes en memoria, comprimidos (cualquier formato de compresión, rar, zjp, cab, arj, arz), ocultos y archivos en ejecución.

El antivirus ofertado deberá además tener la capacidad de detectar y eliminar AdAware y SpyWare.

El antivirus ofertado deberá de tener la certificación CheckMark Spyware para el sistema operativo Microsoft Windows XP.

El antivirus ofertado deberá de tener un modulo residente, ejecutando en la memoria del sistema o comunmente llamado scanner "on-access" y un modulo de revisión antivirus ejecutado en forma manual por el usuario o comunmente llamado scanner "on-demand".

El scanner "on-access" no se podrá desactivar, a menos que tenga la contraseña autorizada.

El antivirus ofertado deberá de tener un componente que busque virus en el protocolo POP3, descarga de e-mails y HTTP, navegación en Internet.

El antivirus ofertado deberá de tener un componente que proteja al usuario de macro-virus en documentos MS Office.

Servidor de Archivos y/o Aplicaciones

El antivirus ofertado deberá de soportar los sistemas operativos MS Windows NT Server, MS Windows 2000 Server/ Advanced Server, MS Windows 2003 Server, Novell Netware y Linux.

El antivirus ofertado deberá de detectar virus, troyanos, macro virus, gusano y malware en todos los archivos, o tipos de archivos, residentes en memoria, comprimidos (cualquier formato de compresión, rar, zip, cab, arj, arz), ocultos y archivos en ejecución.

El antivirus ofertado deberá además tener la capacidad de detectar y eliminar AdAware y SpyWare en los sistemas operativos MS Windows y Linux.

El antivirus ofertado deberá de tener un modulo residente, ejecutando en la memoria del sistema o comunmente llamado scanner "on-access" y un modulo de revisión antivirus ejecutado en forma manual por el usuario o comunmente llamado scanner "on-demand".

El antivirus ofertado para los servidores de archivos Linux deberá tener las siguientes certificaciones:

MINISTERIO DE SALUD
HOSPITAL "VICTOR LARCO HERRERA"
Sr. EDGAR TUESTA RAMOS
Director de la Oficina de Estadística e Informatica

- **"Red Hat Ready Partner"** en la categoría de aplicaciones de "Seguridad" para el sistema operativo Red Hat Enterprise Linux 4 y 5 (plataforma x86).
- **"Novell Technology Partner"** en la categoria Software: Antivirus para el sistema operativo SUSE Linux Enterprise Server 9 y 10(plataforma x86).

Consola de Administración Centralizada

La consola deberá de actualizarse automáticamente manteniendo la seguridad de la red.

La consola deberá de manejarse centralizadamente desde múltiples lugares y redes locales a través de la red.

La consola deberá de proveer informes automáticos y personalizables que permitan supervisar las actividades del antivirus.

La consola deberá de permitir la configuración remota de la solución ofertada en las estaciones de trabajo cliente y servidores de aplicaciones y/o datos cliente.

La consola deberá de buscar los ordenadores y/o servidores desprotegidos en la red.

La consola deberá de permitir la distribución de carga incrementando la escalabilidad del sistema.

La consola deberá de admitir múltiples métodos de instalación remota, en línea o fuera de línea, en la instalación del antivirus para las estaciones de trabajo cliente.

Servidor de Correo Linux

La solución ofertada deberá de incluir los siguientes servicios de seguridad tales como antivirus, antispam, filtro de contenido, inspección profunda del cuerpo del correo electrónico y de los archivos adjuntos, etc.

La solución ofertada permitirá incorporar las tecnologías de revisión **"open source"** y comerciales.

La solución ofertada deberá incluir un motor de políticas que le proporciona al administrador de red la flexibilidad de aplicar diferentes servicios de seguridad de correo electrónico a cualquier número de usuarios finales de acuerdo a sus direcciones, dominios, etc.

La solución ofertada deberá incluir varias características de seguridad tales como protección DoS, blacklisting, protección mail-bomb, etc.

La solución ofertada deberá de soportar etiquetar firmas, marcador de cabezeras, marcador de asunto, etc

MINISTERIO DE SALUD
HOSPITAL "VICTOR LARCO HERRERA"
Dr. EDGAR TUESTA RAMOS
Jefe de la Oficina de Estadística é Informática

La solución ofertada deberá de soportar múltiples motores de revisión de virus.

La solución ofertada deberá de incluir como máximo 4 motores.

La solución ofertada deberá de incluir un filtro de contenido para correo electrónico.
La solución ofertada deberá de incluir un extensivo SNMP MIB para monitorear la tasa de correo electrónico, volumen, spam, virus, los mas grandes remitentes, los mas grandes receptores, estadísticas por motor, etc.

La solución ofertada deberá de incluir un grupo de funciones utilitarias tales como disclaimers, lista de controles de acceso, RBLs por grupo, inspección profunda del cuerpo del correo electrónico, limitaciones del tamaño de los archivos adjuntos, etc.

La solución ofertada deberá remover cualquier parte MIME de un correo electrónico basado en nombres, tipo, tamaño u otro criterio y colocar esa parte MIME en un servidor http o ftp y referir la sección MIME de un correo electrónico con un enlace directo.

La solución ofertada deberá de alertar cuando los remitentes y receptores están enviando una gran cantidad de correos electrónicos o spam.

El antivirus ofertado no deberá de recurrir a librerías, scripts o programas externos.

El antivirus ofertado deberá de descomprimir los archivos adjuntos comprimidos sin necesidad de recurrir a programas externos.

El antivirus ofertado deberá de tener algún mecanismo de notificación a los administradores de red.

El antivirus ofertado deberá de tener la opción de escribir información sobre infiltraciones dentro del encabezado, pie y asunto del mensaje.

El antivirus ofertado deberá de tener certificaciones.

- **"Red Hat Ready Partner"** en la categoría de aplicaciones de "Seguridad" para el sistema operativo Red Hat Enterprise Linux 4 y 5 (plataforma x86).
- **"Novell Technology Partner"** en la categoria Software: Antivirus para el sistema operativo SUSE Linux Enterprise Server 9 y 10(plataforma x86).

PLAZO DE ENTREGA

La entrega de las licencias de software no deberá exceder de los tres días calendarios, desde la emisión de la Orden de Compra.

CAPACITACIÓN

MINISTERIO DE SALUD
HOSPITAL "VICTOR LARCO HERRERA"

Sr. EDGAR TUESTA RAMOS
Director de la Oficina de Estadística e Informática

Se deberá ofrecer un programa de adiestramiento técnico-teórico-práctico para el personal de Informática de la ENTIDAD, con el propósito de capacitarlos en la administración, configuración, monitoreo y mantenimiento adecuado del software.

SERVICIOS ADICIONALES

- Soporte técnico local 24 horas del día por 7 días de la semana por 365 días del año.
- Soporte técnico en la ENTIDAD con un tiempo de respuesta no mayor de 3 horas.
- Plan de contingencia en caso el Antivirus contratado no pueda eliminar un nuevo Virus.

8. ANALISIS COMPARATIVO COSTO.

El Precio de la licencia Corporativa hasta 300 equipos por año es:

McAfee	Precio: S/120.00 + I.G.V. p/licencia.
ESET NOD32	Precio: S/.100.00 + I.G.V. p/licencia.
Kaspersky	Precio: S/.130.00 + I.G.V. p/licencia.

El precio presentado es para un rango hasta 300 equipos aproximadamente.

9. CONCLUSIONES

- Se determinó los características técnicas mínimas que deben ser consideradas para la adquisición del software antivirus.
- Se realizo el análisis comparativo de costo en base a una cantidad referencial.

Andrés Emerson Quiroz López

Soporte Técnico
HVLH