EsSalud
Humanizando el Seguro Social

"Año de la consolidación del Mar de Grau"
"Año de la Conmemoración del Octogésimo Aniversario de la Creación de la Seguridad Social en el Perú"

80 años EsSalud Unidos para ti 1936 - 2016

INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE ANTIVIRUS

INFORME TÉCNICO N° 524 SGST-GPROD-GCTIC-ESSALUD-2016/LRR

1. **NOMBRE DE LA OFICINA**

   El área encargada de la evaluación técnica para la adquisición de software es la Gerencia Central de Tecnologías de Información y Comunicaciones.

2. **RESPONSABLE DE LA EVALUACION**
   Ing. Larry Riega Riega

3. **CARGO**
   Administración Antimalware.

4. **FECHA**
   30 de Marzo 2016

5. **JUSTIFICACION**

   EsSalud requiere la adquisición de licencias antivirus para proteger los activos de información de la institución, utilizados en el otorgamiento de prestaciones a nuestros asegurados.

   La infraestructura tecnológica de la institución está en riesgo de todo tipo de ataques cibernéticos, requiriendo de una herramienta que realice la detección en forma pasiva en combinación con detección activa y bloqueo en el punto de monitoreo que permitirá detener amenazas de malware, disponer de elementos que brinden métodos de remediación en el caso de infección y administrar reportes que permitan tomar decisiones adecuadas al personal de seguridad de la información de EsSalud.

   Por lo expuesto y en el marco de la Ley 28612 "Ley que norma el uso, adquisición y adecuación del software en la Administración Pública" , se procede a evaluar el software antivirus.

6. **ALTERNATIVAS**

   Considerando los requerimientos de EsSalud se ha revisado el mercado nacional en busca de respuestas al requerimiento corporativo, en ese sentido , se ha tomado conocimiento de las funcionalidades de las siguientes marcas:

   - Sophos Endpoint Security and Control.
   - Symantec Endpoint Protection
   - Kaspersky Endpoint Security

7. **ANÁLISIS COMPARATIVO TECNICO**

   El análisis comparativo técnico se basará en la metodología establecida en la "Guía Técnica sobre evaluación de software para la Administración Pública" (R.M. N° 139-2004-PCM) , en función a lo establecido en el reglamento de la ley N° 286126.

SUB GERENCIA DE SOPORTE TECNICO V°B° L. DIAZ V. SUB GERENTE GCTIC-ESSALUD

7.1 Propósito de evaluación
Definir si las opciones evaluadas reúnen las funcionalidades técnicas encomendadas.

7.2 Identificar el tipo de producto
Software de Antivirus Institucional.

7.3 Identificación del modelo de calidad
Para la evaluación técnica del Software Antivirus Institucional se va a utilizar la guía de evaluación de software aprobado por Resolución Ministerial N° 139-2004-PCM.

7.4 Selección de Métricas
Las métricas fueron identificadas de acuerdo a los criterios de las especificaciones técnicas de EsSalud, revisar Anexo 01.

8. ANALISIS COMPARATIVO DE COSTO - BENEFICIO

Para el análisis costo beneficio se evaluaron una diversidad de aspectos relevantes a la contratación, como la funcionalidad, portabilidad, fiabilidad, capacidad de mantenimiento, eficiencia y usabilidad.

Los costos son referenciales, revisar anexo 02.

9. CONCLUSIONES

En función al estudio de costo beneficio efectuado, este informe concluye que la solución Kaspersky Total Security for Business, reúne todas las funcionalidades y características requeridas, pero es importante precisar que todos los productos evaluados cumplen con los requerimientos técnicos estipulados.

10. FIRMA

Larry RIEGA RIEGA
07266365.

EsSalud
Humanizando el Seguro Social

"Año de la consolidación del Mar de Grau"
"Año de la Conmemoración del Octogésimo Aniversario de la Creación de la Seguridad Social en el Perú"

80 años EsSalud Unidos para ti 2020 - 2021

ANEXO 01

CARACTERISTICAS TECNICAS DE SOFTWARE ANTIVIRUS INSTITUCIONAL

	Descripción	Puntaje	Kaspersky	Symantec	Sophos
FUNCIONALIDAD	Deberá contar con un sistema de protección en la navegación web, basado en la reputación de sitios web que permitan de manera proactiva bloquear y evitar que los usuarios ingresen y descarguen componentes maliciosos e infecten sus estaciones.	Total : 4 Parcial : 2 Nada . 0	4	4	4
	La solución de protección para las estaciones no solo estará estructurada en detección de firmas, deberá también estar basada en detección proactiva por comportamiento.	Total : 4 Parcial : 2 Nada . 0	4	4	4
	La solución deberá incluir un sistema para el control de aplicaciones que permita controlar y bloquear el uso de aplicaciones cliente que causan impacto negativo en el trabajo de los usuarios, las mismas que deben ser categorizadas por el postor en forma automática y mensual.	Total : 4 Parcial : 2 Nada . 0	4	4	4
	Deberá bloquear en forma proactiva todo tipo de amenazas de malware como ransonware, Criptovirus ó secuestradores de información en cualquiera de sus variantes, amenazas persistentes avanzadas, polimorfismo, ataques Zero-Day y amenazas de malware desconocidas que no están basadas en firmas.	Total : 4 Parcial : 2 Nada . 0	4	4	2
	La solución ofertada deberá mostrar las actualizaciones pendientes de aplicar a los equipos de la red clasificados por nombre de actualización, grupos de equipos o clasificados por tipo de actualización ó forma de reporte para una mejor y rápida atención.	Total : 4 Parcial : 2 Nada . 0	4	4	4
	La solución ofertada deberá contar con un componente que permita protección en tiempo real, para su correo electrónico, así como su integración con Microsoft Outlook 2000 ó superior, permitiendo decidir el tipo de correo que se desea escanear: Entrante, Saliente ó ambos. También debe de incluir la protección antiphishing, esta solución deberá ser implementada a nivel de servidor de correo.	Total : 2 Parcial : 1 Nada . 0	2	2	2
	La solución incluye una tecnología de detección de intrusos de host (IDS) o prevención de intrusos de host (HIPS) incorporado en el agente antimalware que brinde protección en acceso. Es decir, no deberá ser necesario instalar ningún componente adicional como firewalls personales para poder activar esta funcionalidad.	Total : 4 Parcial : 2 Nada . 0	4	4	4
	El producto deberá ser capaz de evitar que sus procesos, servicios ó archivos de registro puedan ser detenidos, deshabilitados, eliminados ó modificado, para que de esta manera se pueda garantizar su funcionamiento ante cualquier tipo de ataque de malware.	Total : 4 Parcial : 2 Nada . 0	4	4	4
	La solución ofertada deberá evitar una infección provocada por la ejecución del archivo Autorun.Inf contenido en un dispositivo de USB al momento de ser conectado a la estación de trabajo, así mismo deberá evitar que los archivos dentro de los medios extraíbles se oculten o modifiquen por acción de cualquier malware.	Total : 4 Parcial : 2 Nada . 0	4	2	2
	Deberá realizar análisis proactivo de amenazas en base a comportamientos sospechosos de las aplicaciones desconocidas proporcionando una detección más precisa del software malicioso y sus variantes.	Total : 4 Parcial : 2 Nada . 0	4	4	4
	Deberá incorporar un sistema DLP o Data Loss Prevention para evitar que los datos se lleven a unidades USB, y otros dispositivos de almacenamiento extraíbles; puede poder especificar qué dispositivos autorizados pueden usarse y cuáles no de conformidad con cualquiera de los parámetros basados en Windows para este tipo de dispositivos. La solución ofertada, integrará nativamente una opción que permitirá bloquear los medios extraíbles, detectando para ello el tipo y modelo de dispositivo el cual deberá ser reportado a la consola principal.	Total : 4 Parcial : 2 Nada . 0	4	4	4
	Subtotal		46	44	42

SUB GERENCIA SOPORTE TECNICO V°B° L. DIAZ V. SUB GERENTE OGTIC-ESSALUD

	Descripción	Puntaje	Kaspersky	Symantec	Sophos
PORTABILIDAD	La consola de administración deberá mantener una base de datos interna o externa en la cual se almacenará en tiempo real toda la información relacionada a la actividad en la plataforma antivirus (despliegue, instalación, actualización, monitoreo), así como deberá incluir el soporte para bases de datos estándares del mercado (Oracle ó Microsoft SQL Server por ejemplo). Debe incluir el motor de base de datos con el que trabaja.	Total : 4 Parcial : 2 Nada . 0	4	4	4
	La consola deberá poder detectar estaciones de trabajo nuevas en el Active Directory, subnets, cualquier grupo de trabajo ó rango de direcciones ip y debe verificar si tiene el antivirus instalado, si no lo tiene, instalar el antivirus automáticamente de forma remota e importarlas inmediatamente a su grupo correspondiente, previamente definido. Bajo ningún motivo las estaciones permanecerán en un grupo sin asignar por más de una hora. No se agruparán a su correspondiente grupo en forma manual.	Total : 4 Parcial : 2 Nada . 0	4	4	2
	La consola de administración deberá tener un esquema distribuido de repositorios de instalación y debe permitir la activación de múltiples modalidades de actualización, incluyendo transmisión http, ftp o por UNC, que permitan un ahorro de ancho de banda a nivel local y nacional, mientras se efectúan labores de instalación, actualización.	Total : 4 Parcial : 2 Nada . 0	4	4	4
	Deberá permitir la creación de paquetes de instalación personalizados para el antivirus, además de la distribución y actualización del producto.	Total : 2 Parcial : 1 Nada . 0	2	2	2
	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. Las actualizaciones deberán ser totalmente constantes y auditables que eviten la generación de archivos de gran tamaño.	Total : 2 Parcial : 1 Nada . 0	2	2	2
	La consola deberá permitir crear repositorios de firmas y actualizaciones tanto en equipos Windows como Linux, las mismas que deberán ser gestionadas desde la consola.	Total : 4 Parcial : 2 Nada . 0	4	4	4
	Debe permitir administrar la seguridad para Smartphone con soporte para IOS, Android y Windows. Las versiones solicitadas son las siguientes: • IOS 6.0 en adelante. • Android 4.0 en adelante. • Windows Phone 7.0 en adelante.	Total : 4 Parcial : 2 Nada . 0	4	4	4
	La solución para equipos móviles no necesariamente debe estar asociada al uso de la misma consola de administración de la solución de antivirus, pudiendo ser una solución independiente que cumpla con los requisitos solicitados en las bases.	Total : 4 Parcial : 2 Nada . 0	4	4	4
	Deberá permitir el manejo flexible de las licencias de manera que puedan ser reasignadas en caso se cambie de equipo.	Total : 2 Parcial : 1 Nada . 0	2	2	2
FIABILIDAD	La consola de administración debe de permitir realizar un backup, de todas las bases de datos, certificados digitales, llaves de registro, información de parches, configuraciones, políticas realizadas en el sistema y toda información adicional que permita la restauración de la Consola de Administración al punto en que se generó el mismo, sin necesidad de recurrir a programas o scripts externos al producto propuesto. Esta tarea no será realizada por otra aplicación distinta a la Consola de Administración.	Total : 4 Parcial : 2 Nada . 0	4	4	4
	La comunicación será encriptado entre servidores y clientes, usando certificados digitales.	Total : 2 Parcial : 1 Nada . 0	2	2	2
	Subtotal		36	36	34

SUB GERENCIA DE SOPORTE TECNICO V°B° L. DIAZ V. SUB GERENTE GCTIC-ESSALUD

EsSalud
Humanizando el Seguro Social

"Año de la consolidación del Mar de Grau"
"Año de la Conmemoración del Octogésimo Aniversario de la Creación de la Seguridad Social en el Perú"

80 años EsSalud Unidos para ti 1936 - 2016

	Descripción	Puntaje	Kaspersky	Symantec	Sophos
CAPACIDAD DE MANTENIMIENTO	La consola deberá encontrarse implementada en un esquema de alta disponibilidad con posibilidad de redundancia en caso de fallo en la consola principal, configurada en forma automática	Total : 2 Parcial : 1 Nada . 0	2	2	2
	Soporte a servidores de correo bajo plataforma Linux, tales como Postfix y Zimbra, incluyendo versiones en 32 y 64 bits para ambas plataformas.	Total : 2 Parcial : 1 Nada . 0	2	2	2
	Soporte a los servidores de Correo MS Exchange Server 2007, 2010 en adelante, el soporte será brindado a todas las ediciones de los productos y el soporte considera además la configuración en clúster u otra arquitectura en alta disponibilidad.	Total : 2 Parcial : 1 Nada . 0	2	2	2
EFICIENCIA	El software deberá ser considerado como líder en el cuadrante de Gardner para Soluciones de Seguridad Endpoint en los últimos 03 años como mínimo.	Total : 2 Parcial : 1 Nada . 0	2	2	2
	Detectar 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, La tecnología de esta solución le permitirá tomar muestras de posibles archivos y enviarlas automáticamente para su análisis sin necesidad de intervención por parte del usuario	Total : 4 Parcial : 2 Nada . 0	4	4	4
USABILIDAD	La consola deberá tener la funcionalidad de generar usuarios independientes para la administración de determinados segmentos de la red corporativa, los cuales serán definidos por intervalos de direcciones Ip.	Total : 4 Parcial : 2 Nada . 0	4	4	2
	La solución ofertada incluirá alguna utilidad que realice un análisis detallado y a través del mismo reportar un diagnóstico profundo de la estructura del sistema, como librerías, aplicaciones instaladas, claves de registro entre otras, que puedan tener un comportamiento sospechoso como consecuencia del ataque de algún malware.	Total : 2 Parcial : 1 Nada . 0	2	2	2
	Subtotal		18	18	16
	Total		100	98	92

SUB GERENCIA DE SOPORTE TECNICO V°B° L. DIAZ V. SUB GERENTE GCTIC-ESSALUD

ANEXO 02

Costos Referenciales de licencia y mantenimiento por 02 meses

Software	Costo por Licencia y/o soporte por usuario
Kaspersky Total Security for Business	S/.64.24
Sophos Endpoint Security and Control	S/. 43.75
Symantec Endpoint Protection	NO ENVIO COTIZACION

Análisis Costo Beneficio

Software	Costo Total	Beneficio
Kaspersky Total Security for Business	S/.64.24	100
Sophos Endpoint Security and Control	S/.43.75	92

SUB GERENCIA DE SOPORTE TECNICO V°B° L. DIAZ V. SUB GERENTE GCTIC-ESSALUD