

“Sustento Técnico para la Adquisición de Licencias de Software Antivirus”

Nombre del área : Oficina de Tecnologías de la Información

Responsables de la Evaluación : Richard Reynaldo Huamán Mezarina
Asistente en Infraestructura Tecnológica

Fecha : 03 de noviembre 2020

1. Justificación

La Central de Compras Públicas – PERÚ COMPRAS requiere proteger la información digital, almacenada en los equipos informáticos de la institución, de ser alterada, eliminada o copiada sin previo conocimiento del usuario responsable; mediante el empleo de programas no deseados como virus informáticos, troyanos, spyware y la serie de variantes de los mismos.

2. Alternativas de evaluación

Para la selección de alternativas, se tomó como base a los fabricantes de soluciones líderes, según el Cuadrante Mágico de Gartner, que tuvieran por lo menos un representante autorizado en el Perú. Las alternativas seleccionadas se muestran a continuación:

FABRICANTE	PRODUCTO
Kaspersky	Kaspersky Endpoint Security Cloud Plus
Eset	Eset Secure Busines Cloud
Symantec	Symantec Endpoint Protection Cloud
Seqrite	Endpoint Security Cloud

3. Análisis comparativo técnico

El análisis técnico ha sido realizado en conformidad con la metodología establecida en la “Guía Técnica sobre evaluación de software en la Administración Pública”.

Identificador de tipo de producto: Software de protección contra programas no deseados (virus informáticos, troyanos, spyware, etc.).

Selección de métricas: Las métricas se seleccionaron en base a las necesidades de la Institución y a antecedentes previos de evaluación para este tipo de software en el sector Público Peruano.

MODELO DE CALIDAD		
ÍTEM	ATRIBUTO	DESCRIPCIÓN
MÉTRICAS INTERNAS		
1	Sistemas operativos de estaciones de trabajo	Microsoft Windows 8.1 Professional y Microsoft Windows 10 Professional. En versiones de 32 y 64 bits.
2	Plataforma de administración	Cloud
3	Protección para computadoras de escritorio y servidores.	Debe entregar protección avanzada contra malware, spyware, adware, keyloggers para computadoras de escritorio y servidores de archivos.
4	Cortafuegos - Firewall	Bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

“Sustento Técnico para la Adquisición de Licencias de Software Antivirus”

5	Control de Acceso a Dispositivos	Control de Acceso a Dispositivos para administrar el uso de los dispositivos portátiles (memorias USB, discos duros USB, CDs, DVDs, etc.). Permite opciones de bloquear, solo lectura, escritura. Genera reportes del uso. Integrado con el Directorio Activo de Microsoft Windows Server 2012 R2.
6	Protección contra ataques de día cero.	Las actualizaciones automáticas deben proteger las vulnerabilidades de computadores de escritorio y servidores. El escaneo real al momento de acceso debe impedir proactivamente que malware, programas espía y otros programas no deseados se instalen e infecten sus sistemas.
7	Antivirus para Email	Antivirus, Anti spam y filtro de contenido para Exchange.
8	Seguridad	El antivirus debe ser capaz de evitar que sus procesos, servicios, archivos, o archivos de registro puedan ser detenidos, deshabilitados, eliminados o modificados, para de esta manera garantizar su funcionamiento ante cualquier tipo de ataque de virus.
9	Funcionalidad	El antivirus debe ser capaz de crear exclusiones de escaneo ya sea por archivo, extensión, aplicación específica o malware específico. Debe tener niveles predefinidos de protección. Debe permitir bloquear la ejecución de programas no deseados. Todo el producto a ofertar deberá ser del mismo fabricante.
METRICAS EXTERNAS		
10	Instalación y Actualización	Las instalaciones deberán ejecutarse directamente desde la Consola de Administración del Antivirus, además debe existir la posibilidad de instalación desde un CD o Recurso UNC. Debe contar con un aplicativo para la creación de instalaciones personalizadas. Debe estar basado en arquitectura jerárquica (dominios, grupos de elementos, elementos, otros) con esquema distribuido de repositorios de instalación. Las actualizaciones deberán ser manuales y automáticas (tareas programadas) del fichero de firma de virus y del motor de búsqueda en los servidores y estaciones de trabajo de Internet de forma centralizada desde la consola de administración. Debe brindar la creación y administración de repositorios distribuidos y programados.
11	Administración de seguridad simplificada	Debe contar con una sola consola que permita administrar la seguridad (antivirus, software contra programas espía, desktop firewall, prevención de intrusos, control de acceso), con capacidad de despliegue, instalación, desinstalación, actualización y monitoreo. Debe permitir la creación y configuración de grupos de equipos y la aplicación de distintas directivas (políticas) y tareas por grupo de equipos a través de la consola de administración. La consola debe permitir delegar su administración, basado en roles.
12	Compatibilidad	Si la solución antivirus necesita de una base de datos externa, el proveedor deberá entregar las licencias requeridas para su funcionamiento y realizar la instalación, administración y mantenimiento de tal manera que pueda asegurar su operación.
13	Manejo de Licencias	El software debe de permitir un manejo flexible, de manera que puedan ser reasignadas en caso se cambie de equipo.
ATRIBUTOS DE USO		
14	Alertas y Reportes	La consola de administración deberá ser capaz de notificar los eventos de virus a través de diferentes medios (correo electrónico, alertas de registro, etc.) Además generar reportes gráficos tipo barra, pastel, imprimibles y exportables, de la cobertura de versiones, actualizaciones e infecciones
15	Facilidad de Uso y Capacitación	El software antivirus debe ser rápido y de fácil uso. Se deberá considerar la capacitación al personal responsable de la administración del antivirus en la INSTITUCION.
16	Soporte técnico	El Software debe de contar con soporte y mantenimiento por el plazo mínimo de 12 meses. Soporte del fabricante 08 horas del día, los 5 días de la semana (8 x 5) (Tiempo de respuesta de 1hr). Soporte del Partner local on-site del tipo 8x5 (Tiempo de respuesta de 4hr).
17	Documentación	El sistema deberá contar con todos los manuales que permitan su instalación y configuración.

“Sustento Técnico para la Adquisición de Licencias de Software Antivirus”

Niveles y escalas para las características o funcionalidades: Se ha establecido la siguiente escala para la valoración de cada atributo definido en el modelo de calidad

Modelo de Calidad		Escala		
Ítem	Atributo	Puntajes Válidos	Máxima Aprobatoria	Mínimo Aprobatoria
MÉTRICAS INTERNAS				
1	Sistemas operativos de estaciones de trabajo	0 = No cumple 5 = Cumple	5	5
2	Plataforma Cloud	0 = No cumple 5 = Cumple	5	5
3	Protección para computadoras de escritorio y servidores.	0 (mínimo) al 8 (máximo), de acuerdo al nivel de protección brindado.	8	6
4	Cortafuegos – Firewall	0 (mínimo) al 8 (máximo), de acuerdo a la funcionalidad brindada.	8	6
5	Control de Acceso a Dispositivos	0 (mínimo) al 8 (máximo), de acuerdo a las opciones de bloqueo ofrecidas.	8	6
6	Protección contra ataques de día cero.	0 (mínimo) al 8 (máximo), de acuerdo a las opciones de protección ofrecidas.	8	6
7	Antivirus para Email	0 = No cumple 7 = Cumple	7	5
8	Seguridad	0 = No cumple 7 = Cumple	7	5
9	Funcionalidad	0 (mínimo) al 7 (máximo), de acuerdo al grado de cumplimiento de las especificaciones establecidas.	7	5
MÉTRICAS EXTERNAS				
10	Instalación y Actualización	0 (mínimo) al 7 (máximo), de acuerdo al grado de cumplimiento de las especificaciones establecidas.	7	6
11	Administración de seguridad simplificada	0 (mínimo) al 5 (máximo), de acuerdo a las funcionalidades ofrecidas a través de la consola de administración.	5	5
12	Compatibilidad	0 = No cumple 5 = Cumple	5	5
13	Manejo de Licencias	0 (mínimo) al 3 (máximo), de acuerdo a la flexibilidad en la gestión de licencias.	3	2
ATRIBUTOS DE USO				
14	Alertas y Reportes	0 (mínimo) al 5 (máximo), de acuerdo al grado de cumplimiento de las especificaciones establecidas.	5	5
15	Facilidad de Uso y Capacitación	0 (mínimo) al 5 (máximo), de acuerdo al grado de cumplimiento de las especificaciones establecidas.	5	5
16	Soporte técnico	0 = No cumple 5 = Cumple	5	5
17	Documentación	0 = No cumple 2 = Cumple	2	1
TOTAL			100	83

“Sustento Técnico para la Adquisición de Licencias de Software Antivirus”

Modelo de Calidad		Escala	Productos Evaluados			
Ítem	Atributo	Puntajes Máximo	Kaspersky Endpoint Security Cloud Plus	Eset Secure Business Cloud	Symantec Protection Suite Enterprise Edition	Seqrite Endpoint Security Cloud
MÉTRICAS INTERNAS						
1	Sistemas operativos de estaciones de trabajo	5	5	5	5	5
2	Sistemas operativos de servidores de Red	5	5	5	5	5
3	Protección para computadoras de escritorio y servidores.	8	8	8	8	8
4	Cortafuegos - Firewall	8	8	8	8	8
5	Control de Acceso a Dispositivos	8	8	8	8	8
6	Protección contra ataques de día cero.	8	8	8	8	8
7	Antivirus para Email	7	7	7	7	7
8	Seguridad	7	7	7	7	7
9	Funcionalidad	7	7	7	7	7
MÉTRICAS EXTERNAS						
10	Instalación y Actualización	7	7	7	7	7
11	Administración de seguridad simplificada	5	5	5	5	5
12	Compatibilidad	5	5	5	5	5
13	Manejo de Licencias	3	3	3	3	3
ATRIBUTOS DE USO						
14	Alertas y Reportes	5	5	5	5	5
15	Facilidad de Uso y Capacitación	5	5	5	5	5
16	Soporte técnico	5	5	5	5	5
17	Documentación	2	2	2	2	2
Total		100	100	100	100	100

Tomando el cuadro como referencia, todas las soluciones antivirus presentadas cumplen con los atributos o especificaciones mínimas.

Este análisis tiene un peso del 80%. De esta manera, se han evaluado las características técnicas de los productos mencionados y servicios adicionales, habiéndose verificado que cada uno de ellos cubre nuestras necesidades.

“Sustento Técnico para la Adquisición de Licencias de Software Antivirus”

Propósito de la Evaluación: Cuantificar el nivel de cumplimiento de las alternativas seleccionadas respecto a los requerimientos funcionales y técnicos de la Central de Compras Públicas - PERÚ COMPRAS.

4. Análisis comparativo de costo - beneficio

El software deberá incluir la actualización permanente de las herramientas y elementos que componen la solución. Todos los productos ofrecidos DEBEN corresponder a las últimas versiones.

	Kaspersky Endpoint Security Cloud Plus	Eset Secure Business Cloud	Symantec Protection Suite Enterprise Edition	Seqrite Endpoint Security Cloud
Adquisición de 22 licencias	2,218.92	2,976.60	1,713.80	1623.60
Instalación y Puesta en Producción	Incluida	Incluida	Incluida	Incluida
Capacitación	Incluida	Incluida	Incluida	Incluida
Soporte y Mantenimiento externo	Incluida	Incluida	Incluida	Incluida
Personal y Mantenimiento interno	Costo Hundido *	Costo Hundido *	Costo Hundido *	Costo Hundido *
Sub Total	2,218.92	2976.60	1,713.80	1623.60
IGV	487.08	653.40	376.20	356.40
Total	2,706.00	3,630.00	2,090.00	1,980.00
Costo Promedio por Licencia	123	165	95	90
Este análisis tiene un peso del 20 %				
* Los precios se obtuvieron del portal de las marcas ofertadas				

A continuación, se presenta el cuadro N° 3, el resultado global del análisis técnico y el análisis costo beneficio:

ITEM	Atributo	Kaspersky Endpoint Security Cloud Plus	Eset Secure Business Cloud	Symantec Protection Suite Enterprise Edition	Seqrite Endpoint Security Cloud
1	Análisis Comparativo Técnico	80	80	80	80
2	Análisis Costo – Beneficio	18	16	19	20
TOTAL		98	96	99	100

“Sustento Técnico para la Adquisición de Licencias de Software Antivirus”

5. Conclusiones

Por lo cual podemos concluir que las herramientas analizadas cumplen con los requisitos técnicos mínimos, por lo tanto, se recomienda realizar un proceso por concurso en el que participen estas herramientas además de cualquier otra que satisfaga los requerimientos técnicos mínimos.

Richard Reynaldo Huaman Mezarina

Asistente en Infraestructura
Tecnológica

Sergio Andres Guevara Paucar

Coordinador en Infraestructura Tecnológica y
Base de Datos

Jesus De Souza Castro

Jefe de la Oficina de Tecnológicas de la
Información