INFORME TECNICO PREVIO DE EVALUACIÓN DE SOFTWARE ANTIVIRUS INSTITUCIONAL

INFORME TECNICO N° 152 - 2014-MED-SPE-OFIN

1. NOMBRE DE LA OFICINA
   Oficina de Informática

2. RESPONSABLE DE LA EVALUACIÓN
   Jackeline Melgarejo

3. CARGO
   Especialista de IT

4. FECHA
   Marzo 2014

5. JUSTIFICACIÓN

El Ministerio de Educación busca garantizar la continuidad de la adecuada protección de la información almacenada en los equipos de los sistemas informáticos, mediante una solución de antivirus contra programas no deseados como virus informáticos, gusanos, troyanos, spywares, adware, malware y la serie de variantes de los mismos.

Teniendo en cuenta las amenazas cada vez más crecientes de ataques informáticos es necesario considerar funcionalidades específicas para mitigar los riesgos con que actúan los software de código malicioso-malware.

Actualmente el Ministerio de Educación cuenta con el antivirus Kaspersky Endpoint Security cuyas licencias están próximas a vencer. Por ello se requiere contar con software de antivirus que cumpla con los requerimientos técnicos mínimos solicitado por la institución, debido a que es una entidad que tiene impacto nacional.

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 de Diagramación.

6. ALTERNATIVAS

Considerando los requerimientos del Ministerio de Educación se ha buscado alternativas de software en el mercado que cumplan con los requerimientos mínimos, tomando en consideración las necesidades de la entidad. En ese sentido, se consideró los siguientes productos de software a evaluar:

- KASPERSKY ENDPOINT SECURITY.
- SYMANTEC ENDPOINT PROTECTION.
- SOPHOS ENDPOINT PROTECTION AVANZADO.

7. ANALISIS 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" (R.M. N° 139-2004-PCM) tal como se exige en el reglamento de la Ley N° 28612.

7.1. Propósito de evaluación

Validar que las alternativas seleccionadas sean las más convenientes para el Ministerio de Educación.

7.2. Identificar el tipo de producto

Software 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 del Ministerio de Educación, ver Anexo 01.

8. ANALISIS COMPARATIVO DE COSTO – BENEFICIO

El presente análisis tiene por objetivo seleccionar la mejor alternativa. Para lo cual se ha optado por dar un peso a la evaluación técnica de 0.7 y a la evaluación económica de 0.3, con el fin de garantizar que el software a adquirir cumpla con las necesidades mínimas solicitadas.

Los costos son referenciales e incluyen el costo de licencia y mantenimiento por tres (03) años.

Ver detalles en el Anexo 02.

9. CONCLUSION

De acuerdo a la evaluación realizada de costo/beneficio, se recomienda que con la finalidad de disminuir el impacto que implica la implementación y despliegue de una nueva solución de antivirus en los usuarios finales se continúe con el Antivirus Kaspersky EndPoint Security, sin embargo todas las soluciones evaluadas cumplen con los requerimientos técnicos mínimos solicitados.

10. FIRMAS

Jackeline Melgarejo
Especialista de IT-OFIN
Ministerio de Educación

Antonio Santa Cruz
Coordinador (e) de IT-OFIN
Ministerio de Educación

Bari Gloria
Jefe (e) de la Oficina de Informática
Ministerio de Educación

ANEXO 01

CARACTERÍSTICAS TÉCNICAS DE SOFTWARE ANTIVIRUS INSTITUCIONAL

METRICAS (ATRIBUTOS) INTERNAS Y EXTERNAS								
Nº	Atributos	Descripción	Puntaje Máximo	Criterio de calificación	Puntaje	KASPERSKY ENDPOINT SECURITY	SYMANTEC ENDPOINT PROTECTION	SOPHOS ENDPOINT PROTECTION AVANZADO
1	Funcionalidad	La solución permite la detección en tiempo real que proteja contra: virus, gusanos, troyanos, keyloggers, dialers, adware, spyware, hacktools, rootkits, bots, spam, herramientas de control remoto y otros programas potencialmente peligrosos.	4	Todas Algunas Ninguna	4 2 0	4	4	4
		La solución de protección End Point no está solo basada en detección de firmas, sino también en comportamiento, heurística y reputación de archivos y web basada en una nube privada dedicada a proteger proactivamente de malware e infecciones, sean conocidas en la base de firmas o sin estar contenidas en su base de firmas.	4	Todas Algunas Ninguna	4 2 0	4	4	4
3		Posee tecnología de prevención contra "exploit" que atacan vulnerabilidades de aplicaciones como: Adobe, Java, Internet Explorer, File Sharing, Instant Messenger, Mail Client, SSL Client, Web Browser, SQL y servicios de Microsoft.	2	Si No	2 0	2	2	2
4		Debe contar con una tecnología de prevención y detección de intrusos que detecta malware "antes de su ejecución (pre-execution)" y "en ejecución (on-execution)".	2	Si No	2 0	2	2	2
5		Debe detectar, analizar y eliminar, de forma automática y en tiempo real, los programas maliciosos como: Procesos que se ejecutan en la memoria principal (RAM); archivos comprimidos de forma automática, al menos en los siguientes formatos: ZIP, EXE, ARJ, MIME / UU, CAB de Microsoft, Microsoft Comprimir; archivos recibidos a través de software de comunicación instantánea (Chat de Facebook, Skype, Yahoo Messenger, Google Talk, ICQ, entre otros).	4	Todas Algunas Ninguna	4 2 0	4	4	4
6		El producto debe ser capaz de revisar llaves específicas del registro del sistema operativo e impedir intentos de modificación de los componentes del antivirus.	2	Si No	2 0	2	2	2
7		El producto 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.	4	Todas Algunas Ninguna	4 2 0	4	4	4
8		La solución deberá evitar una infección provocada por la ejecución del archivo Autorun.inf contenido en un dispositivo de USB al momento de ser conectado en la estación de trabajo.	2	Si No	2 0	2	2	2
		Debe evitar o monitorear que un programa con comportamiento sospechoso pueda: Incrustar elementos "plug-ins" en el navegador de internet Explorer; instale nuevos servicios; modifique archivos de	2	Todas Algunas Ninguna	2 1 0	2	2	2

METRICAS (ATRIBUTOS) INTERNAS Y EXTERNAS								
Nº	Atributos	Descripción	Puntaje Máximo	Criterio de calificación	Puntaje	KASPERSKY ENDPOINT SECURITY	SYMANTEC ENDPOINT PROTECTION	SOPHOS ENDPOINT PROTECTION AVANZADO
		sistema; instale servicios o programas para iniciarse al arrancar la estación de trabajo.						
10		El sistema de control de aplicaciones permite controlar y bloquear el uso de aplicaciones cliente que causan impacto negativo en el trabajo de los usuarios.	2	Si No	2 0	2	2	2
11		La solución incluye un firewall personal del mismo fabricante administrado centralizadamente desde la consola de gestión. Este firewall permite bloquear, autorizar aplicaciones y puertos específicos tanto local como centralizadamente y permitir creación de reglas por dirección IP, MAC y/o puerto, tanto para el origen como para el destino.	2	Si No	2 0	2	2	2
13		El análisis de los archivos deberá ser realizado de tres formas como mínimo: análisis en tiempo real, análisis programado, análisis de forma manual.	3	Todas Algunas Ninguna	3 1 0	3	3	3
14		Posee la capacidad de escanear a través de puerto 80, 8080, 443 y permite la protección y bloqueo de manera independiente de medios extraíbles tales como dispositivos de almacenamiento USB, CD/DVD.	2	Si No	2 0	2	2	2
15		Garantiza al usuario la navegación en internet de forma segura y bloquear cualquier descarga dañina, software espía así como enlaces ocultos a otros sitios web dañinos.	2	Si No	2 0	2	2	2
16		Soporte para base de datos estándares del mercado (como Oracle o Microsoft SQL Server). Debe incluir el motor de base de datos con el que trabaja.	2	Si No	2 0	2	2	2
17		Capacidad de: detectar y eliminar virus en Microsoft Outlook, inclusive en texto HTML, archivos adjuntos y de excluir de la exploración archivos, carpetas, procesos.	2	Todas Algunas Ninguna	2 1 0	2	2	2
20		El usuario no puede realizar una configuración particular de la solución a menos que el administrador de la red otorgue privilegios ya sea local o mediante la integración con el directorio activo.	2	Si No	2 0	2	2	2
21		Posee consola de administración maestra y distribuida para instalación, actualización y soporte.	2	Si No	2 0	2	2	2
22		La consola permite: integración con Active Directory, detecte antivirus de terceros, realice desintalación remota de antivirus de terceros, instalación y desinstalación de manera "silenciosa", escaneo de red por directorio activo, red IP o dominios, monitoreo de las estaciones de trabajo, almacenar histórico de eventos, notificación de intento de infecciones, descarga de actualizaciones de necesarias de internet, envío de notificaciones SMTP o SNMP.	3	Todas Algunas Ninguna	3 1 0	3	3	3
23		La consola permite: el manejo flexible de las licencias de manera que puedan ser reasignadas en caso se cambie de equipo y la	2	Todas Algunas Ninguna	2 1 0	2	2	1

MINISTERIO DE EDUCACIÓN Infraestructura Tecnológica OFIN

MINISTERIO DE EDUCACIÓN Infraestructura Tecnológica OFIN

METRICAS (ATRIBUTOS) INTERNAS Y EXTERNAS								
Nº	Atributos	Descripción	Puntaje Máximo	Criterio de calificación	Puntaje	KASPERSKY ENDPOINT SECURITY	SYMANTEC ENDPOINT PROTECTION	SOPHOS ENDPOINT PROTECTION AVANZADO
		gestión del consumo de licencias.						
25		Permite crear reportes personalizados, programados, con capacidad de ser enviado por correo electrónico, envío de alertas de prevención de fallas.	3	Todas Algunas Ninguna	3 1 0	3	3	3
26		Características de hardware para la instalación de clientes y consola.	2	Básico Intermedio Avanzado	2 1 0	2	2	2
27		Debe poder instalarse en: Windows XP, Vista, 7, 8, de 32/64 bits.	2	Todas Algunas Ninguna	2 1 0	2	2	2
28	Fiabilidad	Encontrarse (figurar) en los años 2012 y 2013 en el cuadrante mágico de Gartner para protección de plataforma de punto final.	3	Leaders Visionaries o Challengers Niche players No se encuentra	3 2 1 0	3	3	3
29	Capacidad de mantenimiento	El producto debe contar con actualizaciones compactas e incrementales que eviten la generación de archivos de gran tamaño, evitando de esta manera que pueda impactar de una manera negativa a los recursos de ancho de banda de la red.	2	Si No	2 0	2	2	2
30		La solución deberá actualizar sus firmas por lo menos una (01) vez al día.	2	Más de 1 vez 1 vez	2 0	2	2	2
31	Portabilidad	El producto debe ser capaz de crear discos o CDs de rescate que permitan escanear particiones de Windows FAT y NTFS.	2	Si No	2 0	2	2	2
32		Cuenta con antivirus para celulares que debe permitir proteger los equipos celulares de cualquier malware, con soporte para IOS, Android y Windows.	2	Todas Algunas Ninguna	2 1 0	2	2	2
	Sub Total		68			68	68	67

METRICAS (ATRIBUTOS) DE USO								
1	Eficacia	Eficacia en defender los sistemas contra virus, buffer overflows (o desbordamientos de buffer) y ataques combinados.	3	Muy dinámico Dinámico Estático	3 2 1	3	3	3
2		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.	3	Si No	3 0	3	3	3
3	Productividad	Capacidad para tomar distintas acciones cuando sea detectado un virus o un ataque, limpiar el archivo infectado, moverlo a cuarentena, no tomar acción, eliminar el archivo.	3	Todas Algunas Ninguna	3 1 0	3	3	3
		Afección del rendimiento, la performance y el consumo de memoria de las estaciones de trabajo para el análisis, revisiones y escaneos que la solución haga.	3	Baja Media Alta	3 1 0	3	3	3
4	Seguridad	Capacidad de proteger al usuario de ataques de tipo phishing.	2	Si No	2 0	2	2	2

MINISTERIO DE EDUCACIÓN Infraestructura Tecnológica OFIN

METRICAS (ATRIBUTOS) INTERNAS Y EXTERNAS								
Nº	Atributos	Descripción	Puntaje Máximo	Criterio de calificación	Puntaje	KASPERSKY ENDPOINT SECURITY	SYMANTEC ENDPOINT PROTECTION	SOPHOS ENDPOINT PROTECTION AVANZADO
5		La solución incluye una tecnología de detección de intrusos de host (IDS) o prevención de intrusos a nivel de host (HIPS) incorporado en el agente anti-malware que brinde protección en acceso.	2	Si	2	2	2	2
				No	0			
6	Satisfacción	Es una solución nueva de modo que requiere realizar la instalación y despliegue en cada uno de los usuarios.	12	No	12	12	0	0
				Si	0			
7		Es una interfaz que los usuarios ya conocen.	4	Si	4	4	0	0
				No	0			
	Sub Total		32			32	16	16
		Total	100			100	84	83

MINISTERIO DE EDUCACIÓN Infraestructura Tecnológica OFIN

MINISTERIO DE EDUCACIÓN Infraestructura Tecnológica OFIN

ANEXO 02

Costos Referenciales de licencia y mantenimiento por 3 años.

Software	Costo de Licencia y/o soporte por usuario
KASPERSKY ENDPOINT SECURITY	S/. 67.20
SYMANTEC ENDPOINT PROTECTION	S/. 84.56
SOPHOS ENDPOINT PROTECTION AVANZADO	S/. 47.59

Análisis Costo-Beneficio

Software	Costo Total	Beneficio	Beneficio/Costo
KASPERSKY ENDPOINT SECURITY	S/. 67.20	100	0.91
SYMANTEC ENDPOINT PROTECTION	S/. 84.56	84	0.76
SOPHOS ENDPOINT PROTECTION AVANZADO	S/. 47.59	83	0.88

* Precio referencial de una licencia, en soles, no incluyen IGV.

** Se adjunta la lista de precios referenciales del software indicado.

PROPUESTA ECONÓMICA

Platinum Partner

Calle Las Camelias 185 - San Isidro, Lima, Perú
Telf: 6371200
www.softlinegroup.com.pe

SOFTLINE INTERNATIONAL PERU S.A.C		**EMPRESA:**	**MINISTERIO DE EDUCACION**
Contacto:	Jorge John Trujillo Ramirez	**RUC:**	
Telefono:	51 (01) 6371200	**Atención:**	Jackeline Melgarejo
Móvil	980702592	**NRO. COTIZ.**	**SLPE-JT0213-2014-20**
E-mail	jorge.trujillo@softlinegroup.com	**FECHA :**	13 de Febrero del 2014

LICENCIAMIENTO DE SOLUCION DE ANTIVIRUS A 3 AÑOS					
QTY	N° PARTE	DESCRIPCIÓN	Duracion	PRECIO DE VENTA (US$) UNIT	TOTAL
7000	0E7IOZC0-EI3GH	SYMC ENDPOINT PROTECTION 12.1 PER USER BNDL COMP UG LIC GOV BAND H ESSENTIAL 36 MONTHS	3 años	S/. 84.56	S/. 591,920.00
				Subtotal	**S/. 591,920.00**
				IGV	**S/. 106,545.60**
				Total	**S/. 698,465.60**

CONDICIONES COMERCIALES

Los precios están expresados en **Nuevos Soles. Incluyen IGV**

Tiempo de Entrega Licencias: 1 a 15 días, a partir del día siguiente de colocada la Orden de compra

Forma de pago: Licenciamiento contra entrega, Servicios contra conformidad

Tiempo de validez de Oferta: 30 días útiles

Nota: De estar conforme con nuestra Propuesta Económica, reenvie su O/C o el presente dcocumento firmado dando conformidad a la compra y remitalo al correo de su contacto en Softline International Perú.

PROPUESTA ECONÓMICA

Calle Las Camelias 185 - San Isidro, Lima, Perú
Telf: 6371200
www.softlinegroup.com.pe

SOFTLINE INTERNATIONAL PERU S.A.C

Contacto:	Jorge John Trujillo Ramirez
Telefono:	51 (01) 6371200
Móvil	980702592
E-mail	jorge.trujillo@softlinegroup.com

EMPRESA:	**MINISTERIO DE EDUCACION**
RUC:	
Atención:	Jackeline Melgarejo
NRO. COTIZ.	**SLPE-JT0213-2014-20**
FECHA :	13 de Febrero del 2014

LICENCIAMIENTO DE SOLUCION DE ANTIVIRUS A 3 AÑOS

QTY	N° PARTE	DESCRIPCIÓN	Duracion	PRECIO DE VENTA (US$) UNIT	TOTAL
7000	KL4863DA*TS	Kaspersky Endpoint Security for Business - Select - Base	3 años	S/. 67.20	S/. 470,400.00
				Subtotal	**S/. 470,400.00**
				IGV	**S/. 84,672.00**
				Total	**S/. 555,072.00**

CONDICIONES COMERCIALES

Los precios están expresados en **Nuevos Soles. Incluyen IGV**
Tiempo de Entrega Licencias: 1 a 15 días, a partir del día siguiente de colocada la Orden de compra
Forma de pago: Licenciamiento contra entrega, Servicios contra conformidad
Tiempo de validez de Oferta: 30 días útiles

Nota: De estar conforme con nuestra Propuesta Económica, reenvie su O/C o el presente dcocumento firmado dando conformidad a la compra y remitalo al correo de su contacto en Softline International Perú.

INNOVARE

SOPHOS

INNOVARE E-BUSINESS s.a.c.
Calle Soledad N° 471 - Lima 14

Central (511) 711-9643 / 711-9644
Fax (511) 718-3070
Email licitaciones@innovare.pe
Portal www.innovare.pe

COTIZACIÓN Nº 001-0403/2014-008

Señor (a): Jackeline Melgarejo
Ministerio de Educación

Fecha: 04/mar/2014

Email

Telefono:

ITEM	PRODUCTOS	CANTIDAD	P.V.P. (SIN IGV)	SUB TOTAL (SIN IGV)
1	**SOLUCIÓN ANTIVIRUS CORPORATIVO**	7000	S/. 48.59	S/. 340,147.50
	* Cumplimos con las especificaciones técnicas solicitadas * Marca: SOPHOS * Modelo: ENDPOINT PROTECTION AVANZADO * Soporte x 36 meses			

Forma de Pago: **Contado**
Moneda: **Nuevos Soles**
IGV: **INCLUIDO EN EL PRECIO TOTAL**
Validez Oferta: **30 días calendario**
Garantía: **12 meses**
Plazo de Entrega **Licencias: 7 días | Appliances 60 días**

DISTRIBUIDOR:

Razón Social: INNOVARE E-BUSINESS SAC
RUC: 20475805101
Dirección: JR. SOLEDAD Nº 471 - LINCE
Teléfono: 422-5534 Fax: 422-5534 # 100
Correo Electrónico: LICITACIONES@INNOVARE.PE
CCI BCP S/. : 00219311414905507319