"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año del Bicentenario del Perú: 200 años de Independencia"

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE N° 006-2021-MINEDU/SPE-OTIC
"SOLUCIÓN DE ANTIVIRUS CORPORATIVO PARA EL MINISTERIO DE EDUCACIÓN"

1. NOMBRE DEL ÁREA
Oficina de Tecnología de la Información y Comunicación.

2. RESPONSABLES DE LA EVALUACIÓN
Jackeline Melgarejo Reyes
Jorge Trujillo Ramirez

3. CARGO
Especialista del Área de Comunicaciones y Seguridad Lógica UIT-OTIC.
Coordinador del Área de Comunicaciones y Seguridad Lógica UIT-OTIC.

4. FECHA
Octubre del 2021.

5. JUSTIFICACIÓN
El Ministerio de Educación requiere contar con una solución que permita garantizar la seguridad a nivel endpoint, tanto en los equipos desktop como laptops que forman parte de su parque informático; de tal modo que pueda detectar, analizar y eliminar diferentes tipo de amenazas que intenten atacar a los endpoints como: virus, gusanos, troyanos, spyware, bootnet, malware, ransomware y variantes de los mismos, brindando protección ante todo tipo de amenazas tanto conocidas como desconocidas.

Considerando los nuevos tipos de amenazas que aparecen a nivel mundial, los cuales intentan burlar el mayor número de controles de seguridad, es necesario considerar funcionalidades específicas que permitan mitigar los riesgos de infección o robo de información que ocasionan diferentes tipos de software o archivos con contenido malicioso o que intentan explotar alguna vulnerabilidad, amenazas que puede ingresar por diferentes medios como correo, internet, dispositivos móviles entre otros. Por ello es necesario contar una solución de antivirus robusta, por ser una institución de impacto nacional.

Debido a ello es crucial contar con una solución de antivirus para el Ministerio de Educación, que permita brindar protección a todas sus sedes desconcentradas de la entidad, ubicadas en el ámbito de Lima Metropolitana.

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 realizar la evaluación de la solución de Antivirus Corporativo.

6. ALTERNATIVAS
En base a las necesidades y requerimientos del Ministerio de Educación así como los nuevos esquemas relacionados con la protección de amenazas no solo

conocidas, sino también desconocidas, se ha buscado alternativas de soluciones de antivirus en el mercado local que cumplan dichas necesidades y cuenten con el respectivo soporte técnico local.

Por ello, la solución de antivirus que sea seleccionada debe contener como mínimo las funcionalidades que permitan el mejor esquema de protección tanto para la seguridad informática como para la seguridad de la información que se maneja en el Ministerio de Educación.

Teniendo en cuenta lo mencionado, se ha establecido parámetros mínimos que permitan fortalecer la seguridad de TI en los endpoints, con el fin de velar por la disponibilidad, integridad y confidencialidad de la información de la entidad, como factores que conllevan a una mejor evaluación y que a su vez brinden la calidad mínima necesaria que deben tener este tipo de soluciones. Estos requerimientos se encuentran detallados en el ANEXO 01.

En base a las premisas indicadas y a la información obtenida de los productos que hay en el mercado para soluciones de antivirus, así como de las cotizaciones referenciales proporcionadas por los proveedores con la finalidad de realizar el análisis de costo beneficio, se está evaluando las siguientes marcas que son de tipo propietario:

- ESET (ESET Protect Enterprise).
- FSECURE (FSECURE Endpoint Premium para estaciones OnPremise y FSECURE Endpoint Detection and Response para estaciones Cloud).
- KASPERSKY (Kaspersky Endpoint Security for Business – Advanced y Kaspersky Edpoint Detection and Response Advanced).
- MCAFEE (McAfee MVISION Protect Plus EDR for Endpoint & Advanced Threat Defense).
- SOPHOS (SOPHOS Intercept X Avanzado + EDR).

7. 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” (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

Solución de antivirus corporativo.

7.3. Identificación del modelo de calidad

Para la evaluación técnica del Software antivirus se va a utilizar la guía de evaluación de software aprobada por Resolución Ministerial N° 139-2004-PCM.

7.4. Selección de métricas

Las métricas fueron identificadas de acuerdo a los criterios establecidos en base a las necesidades técnicas del Ministerio de Educación.

Según lo establecido en la guía de evaluación y las necesidades institucionales, se definieron las siguientes métricas así como el puntaje máximo, tal como se muestra a continuación:

N°	Atributos	Puntaje Máximo
ATRIBUTOS INTERNOS Y EXTERNOS		
1	FUNCIONALIDAD	51
2	EFICIENCIA	4
3	CAPACIDAD DE MANTENIMIENTO	4
4	PORTABILIDAD	4
5	FIABILIDAD	21
ATRIBUTOS DE USO		
6	EFICACIA	8
7	PRODUCTIVIDAD	4
8	SEGURIDAD	4
	TOTAL	**100**

El detalle de cada característica que forma parte de los atributos indicados, así como el resultado de la evaluación de los productos en base a las características solicitadas se muestra en el ANEXO 01.

Se considerará como aceptable solo los productos cuyo puntaje total en la evaluación de las características y calidad solicitadas, indicadas en el ANEXO 01, sea superior a 80 puntos.

8. ANÁLISIS COMPARATIVO DE COSTO-BENEFICIO

En relación al análisis comparativo de costo-beneficio, se ha proporcionado un peso del 90% a las características y un 10% a los costos de licenciamiento (Ver ANEXO 02).

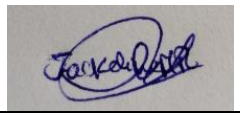
Los costos indicados son solo referenciales, en base a las cotizaciones brindadas por diferentes empresas que se encuentran en el mercado local. Por ello, se precisa que es potestad de la Oficina de Logística realizar el estudio de mercado correspondiente, según la norma vigente.

9. CONCLUSIONES

En base al análisis realizado, se evidencia que de las soluciones de antivirus evaluadas, las correspondientes a las marcas: FSECURE, KASPERSY y MCAFEE obtuvieron un beneficio mayor de 80 puntos que es lo mínimo aceptable, por lo que son las marcas que cumplen tanto con las características técnicas mínimas solicitadas así como la calidad requerida para la protección que corresponde a soluciones de antivirus corporativo que se necesita para el Ministerio de Educación, con la capacidad de brindar la protección a nivel del endpoint tanto para amenazas conocidas como desconocidas y con el fin de cumplir con las normativas de seguridad existentes en la entidad.

Así mismo, la solución de antivirus que obtuvo el mayor puntaje de costo-beneficio fue de la marca KASPERSY.

10. FIRMAS



JACKELINE JOHANA MELGAREJO REYES
Especialista del Área de Comunicaciones y Seguridad Lógica
UIT – OTIC
Ministerio de Educación

JORGE JOHN TRUJILLO RAMIREZ
Coordinador del Área de Comunicaciones y Seguridad Lógica
UIT – OTIC
Ministerio de Educación

FIRMA DIGITAL
Firmado digitalmente por: TRUJILLO RAMIREZ Jorge John FAU 20131370998 soft
Motivo: En señal de conformidad
Fecha: 15/10/2021 23:48:47-0500

ALDO HUMBERTO AMAYA YSLA
Jefe(e) de la Unidad de Infraestructura Tecnológica de la Oficina de Tecnologías de la Información y Comunicación
Ministerio de Educación

FIRMA DIGITAL
Firmado digitalmente por: AMAYA YSLA Aldo Humberto FAU 20131370998 soft
Motivo: En señal de conformidad
Fecha: 15/10/2021 23:54:44-0500

MAX EVER PONCE SOLDEVILLA
Jefe de la Oficina de Tecnologías de la Información y Comunicación
Ministerio de Educación

FIRMA DIGITAL
Firmado digitalmente por: PONCE SOLDEVILLA Max Ever FAU 20131370998 hard
Motivo: Soy el autor del documento
Fecha: 19/10/2021 10:18:53-0500

ANEXO 01

CARACTERÍSTICAS TÉCNICAS DE LA SOLUCIÓN ANTIVIRUS CORPORATIVO PARA EL MINISTERIO DE EDUCACIÓN

N°	Atributos	Descripción	Puntaje Máximo	Criterios de calificación	Puntaje	ESET	FSECURE	KASPERSKY	MCAFEE	SOPHOS
ATRIBUTOS INTERNOS Y EXTERNOS										
1	FUNCIONALIDAD	La solución de seguridad antivirus está basada como mínimo en: a) Detección de firmas, que incluya la protección de amenazas conocidas, b) Análisis de comportamiento, c) Heurística, d) Reputación de archivos y sitios web y e) Aprendizaje automático.	2	Todas:	2	2	2	2	2	2
				Algunas:	1					
2		Brinda protección en base a una nube dedicada a proteger proactivamente todo tipo de amenazas, que incluye: a) Amenazas conocidas y b) Amenazas desconocidas.	2	Todas:	2	2	2	2	2	2
				Algunas:	1					
3		Brinda protección contra todo tipo de amenazas como: Virus, gusanos, troyanos, adware, spyware, bots, phishing, herramientas de acceso remoto, ransomware, programas maliciosos y todo tipo de malware existentes y nuevas variantes.	2	Todas:	2	2	2	2	2	2
				Algunas:	1					
4		Cuenta con tecnología de prevención de intrusos a nivel de host, brindando protección ante cualquier tipo de amenaza, tráfico anómalo o actividad no deseada que perjudique o ponga en riesgo a los equipos.	2	Si:	2	2	2	2	2	2
				No:	1					
5		Permite la protección ante amenazas existentes en: diferentes particiones de disco, unidades de red, medios extraíbles como USB, CD/DVD. Debe evitar todo tipo de infección provocada por la ejecución automática de cualquier tipo de archivo proveniente de un dispositivo USB al momento de ser conectado y sin requerir escaneo previo.	2	Todas:	2	2	2	2	2	2
				Algunas:	1					

N°	Atributos	Descripción	Puntaje Máximo	Criterios de calificación	Puntaje	ESET	FSECURE	KASPERSKY	MCAFEE	SOPHOS
6		Tiene la capacidad de detectar y eliminar amenazas que ingresan por diferentes medios como correo electrónico, usando heurística y otras técnicas de protección solicitadas; inclusive cuando la amenaza se encuentre en texto HTML, enlaces, archivos adjuntos, empaquetados. Debe asegurarse de brindar la protección ante phishing.	2	Todas:	2	2	2	2	2	2
				Algunas:	1					
7		Poseer tecnología de prevención y protección contra "exploit", independientemente del medio por el que intente infectar al equipo.	2	Si:	2	2	2	2	2	2
				No:	0					
8		Firewall: Incluye firewall del mismo fabricante, permitiendo bloquear y autorizar puertos específicos, mediante la creación de reglas por dirección ip, mac, puerto de origen y destino. Todo ello debe tener la capacidad de ser administrado desde la consola EPP.	2	Si:	2	2	2	2	2	2
				No:	0					
9		Control de aplicaciones: Permite identificar aplicaciones instaladas/ejecutadas en los equipos, con el fin de autorizar o bloquear aplicaciones de acuerdo a la necesidad, en base a listas blancas o negras que contienen aplicaciones recomendadas y no recomendadas para uso (según categorías establecidas por el fabricante), así como personalizar el uso o bloqueo de dichas aplicaciones, creando exclusiones a los criterios establecidos por el fabricante. Todo ello debe tener la capacidad de ser administrado desde la consola centralizada del componente EPP.	2	Todas:	2	2	2	2	2	2
				Algunas:	1					

N°	Atributos	Descripción	Puntaje Máximo	Criterios de calificación	Puntaje	ESET	FSECURE	KASPERSKY	MCAFEE	SOPHOS
10		Protección de vulnerabilidades: Cuenta con tecnologías que permita mitigar el riesgo de brindar protección ante la explotación de vulnerabilidades en sistemas operativos y aplicaciones que tengan los equipos clientes. Incluye la aplicación de parches de seguridad de software de diferentes marcas. Todo ello debe tener la capacidad de ser administrado desde la consola centralizada del componente EPP.	2	Todas:	2	2	2	2	2	1
				Algunas:	1					
11		Control web: Permite navegar a internet de forma segura, usando heurística y otras técnicas de protección bloqueando de manera proactiva cualquier descarga dañina, código malicioso, software espía que intenten infectar estaciones de trabajo. Incluye protección web a páginas HTTPS. Muestra mensajes de advertencia sobre la navegación a sitios maliciosos a los que intentan acceder los usuarios. Incluye control web basado en categorías y por reputación y permite personalizar el acceso o bloqueo a determinadas url, creando exclusiones a los criterios establecidos por el fabricante. Todo ello debe tener la capacidad de ser administrado desde la consola centralizada del componente EPP.	2	Todas:	2	2	2	2	2	2
				Algunas:	1					
12		Control de dispositivos: Permite el control (bloqueo y/o habilitación) de dispositivos como mínimos para dispositivos de almacenamiento USB, CD/DVD. Permite la configuración del control de dispositivos para: bloqueo, solo lectura, control total. Dicha configuración puede realizarse por equipo o por usuario. Todo ello debe tener la capacidad de ser administrado desde la consola centralizada del componente EPP.	2	Todas:	2	2	2	2	2	2
				Algunas:	1					

N°	Atributos	Descripción	Puntaje Máximo	Criterios de calificación	Puntaje	ESET	FSECURE	KASPERSKY	MCAFEE	SOPHOS
13		Reportes: Desde la misma consola de administración centralizada del componente EPP se permite crear reportes personalizados, programados, con envío a correo electrónico a cuentas específicas. Estos deben ser exportados como mínimo en formatos: a) HTML, b) PDF, c) csv o excel o xml. Permite envío de alertas de fallas o infecciones. En los reportes se debe visualizar el detalle de los equipos como: nombre de equipo, ip, último usuario conectado, fecha y hora de última conexión. Deben mostrarse el mapeo de los equipos afectados, los cambios que realizaron en los equipos y la afección que esto causa. Dentro de los reportes personalizados deben encontrarse: reportes de amenazas bloqueadas, no bloqueadas, equipos infectados, de equipos con errores con el detalle del error, equipos que no actualizan, sitios web bloqueados, aplicaciones bloqueadas.	2	Todas:	2	2	2	2	2	2
				Algunas:	1					
14		La consola de administración centralizada del componente EPP: Debe ser onpremise para los equipos que se encuentren en las sedes con conexión al MINEDU.	2	Si:	2	2	2	2	2	0
				No:	0					

N°	Atributos	Descripción	Puntaje Máximo	Criterios de calificación	Puntaje	ESET	FSECURE	KASPERSKY	MCAFEE	SOPHOS
15		La consola de administración centralizada del componente EPP debe permitir: monitorear el total de estaciones de trabajo que tienen a su cargo, permitiendo visualizar la información de los equipos administrados como: nombre, ip, dominio, eventos y errores más resaltantes, crear y ejecutar tareas y políticas a grupos así como a equipos específicos, detecta aplicaciones de terceros, tomar acción en caso se detecte equipos infectados, permite el uso de usuarios con diferentes roles de administración, almacena el histórico de eventos de cada equipo administrado, notificar los intentos de infección de amenazas, bloquear cualquier cambio que el usuario intente realizar sobre la configuración de políticas y deshabilitación del antivirus, generación de reportes, permite instalación y desinstalación de la solución antivirus de forma remota con la capacidad de retrasar o suprimir el reinicio, envía notificaciones SMTP o SNMP de los eventos más importantes, permite visualizar el estado de los equipos (activo o inactivo) así como las estadísticas más resaltantes.	5	Todas:	5	5	5	5	5	2
				Algunas:	2					
16		La consola de administración centralizada del componente EPP debe ser capaz de escanear la red por directorio activo. También debe tener la capacidad de escaner segmentos de red configurados.	4	Todas:	4	4	4	4	4	2
				Algunas:	2					
17		Debe contar con el componente de EDR con su propia consola de administración (tanto en el escenario onpremise como en la nube), que permita realizar la detección de las amenazas de día cero, el mapeo de los equipos con eventos y alertas de este tipo, los componentes que están siendo afectados, debe permitir tomar acción sobre estas amenazas detectadas.	5	Onpremise y en nube	5	5	1	5	1	1
				Solo en la nube	1					

N°	Atributos	Descripción	Puntaje Máximo	Criterios de calificación	Puntaje	ESET	FSECURE	KASPERSKY	MCAFEE	SOPHOS
18		Debe contar con el componente de Sandbox con su propia consola de administración (tanto en el escenario onpremise como en la nube), que permita realizar el análisis mediante la detonación de las nuevas amenazas detectadas y tomar acción en base al resultado obtenido.	5	Onpremise y en nube	5	1	1	5	5	1
				Solo en la nube	1					
19		Toda la solución de seguridad antivirus: EPP, EDR y Sandbox deben trabajar en conjunto para brindar protección a los equipos de cómputo.	4	Todas:	4	1	1	4	4	1
				Algunas:	1					
20	EFICIENCIA	La solución de seguridad antivirus: Detecta, detiene, bloquea y evita la instalación, propagación e infección de todo tipo de amenazas.	2	Todas:	2	2	2	2	2	2
				Algunas:	1					
21		Brinda protección aun cuando esta comprometa al sistema operativo y/o aplicación, incluso cuando no existan parches o actualizaciones que cubran dicha vulnerabilidad.	2	Todas:	2	2	2	2	2	2
				Algunas:	1					
22	CAPACIDAD DE MANTENIMIENTO	Permite realizar rollback de firma de virus para casos en los que las firmas generen problemas o incompatibilidades con alguna aplicación específica.	2	Si:	2	2	2	2	2	2
				No:	0					
23		La consola de antivirus centralizada del componente EPP debe tener la capacidad de conectarse automáticamente a internet y descargar las actualizaciones necesarias para todos los productos activados. Dicha conexión deberá poder configurarse en intervalos de tiempo determinados (horas, días).	2	Si:	2	2	2	2	2	2
				No:	0					
24	PORTABILIDAD	La solución de seguridad antivirus es compatible con estaciones de trabajo: Microsoft Windows 8, 8.1, 10 y superiores.	2	Todas:	2	2	2	2	2	2
				Algunas:	1					
25		La consola de administración centralizada del componente EPP debe tener la capacidad de configurar políticas móviles para que cuando un equipo esté fuera de la red institucional, pueda actualizarse vía internet.	2	Si:	2	2	2	2	2	2
				No:	0					

N°	Atributos	Descripción	Puntaje Máximo	Criterios de calificación	Puntaje	ESET	FSECURE	KASPERSKY	MCAFEE	SOPHOS
26	FIABILIDAD	La solución de seguridad antivirus se encuentra en el cuadrante mágico de Gartner para Endpoint tanto de los años 2019 como: Challengers / Visionarios / Líderes.	3	Líderes:	3	1	0	2	2	3
				Visionarios:	2					
				Challengers:	1					
27		La solución de seguridad antivirus se encuentra en el cuadrante mágico de Gartner para Endpoint tanto de los años 2021 como: Challengers / Visionarios / Líderes.	3	Líderes:	3	1	0	2	3	3
				Visionarios:	2					
				Challengers:	1					
28		La solución de seguridad antivirus cuyo resultado promedio de todas las evaluaciones realizadas en el año 2019 (de: febrero, abril, junio, agosto, octubre y diciembre) por AV TEST dirigidas a software antivirus en Sistemas Operativos Windows para empresas, respecto a las 3 categorías (protección, rendimiento y usabilidad), alcanzó una puntuación mayor al 95%.	5	>99%	5	0	5[1]	5	2	1
				>98% y <99%	4					
				>97% y <98%	3					
				>96% y <97%	2					
				>95% y <96%	1					
				<95%	0					
29		La solución de seguridad antivirus cuyo resultado promedio de todas las evaluaciones realizadas en el año 2020 (de: febrero, abril, junio, agosto, octubre y diciembre) por AV TEST dirigidas a software antivirus en Sistemas Operativos Windows para empresas, respecto a las 3 categorías (protección, rendimiento y usabilidad), alcanzó una puntuación mayor al 95%.	5	>99%	5	2	5	5	2	0
				>98% y <99%	4					
				>97% y <98%	3					
				>96% y <97%	2					
				>95% y <96%	1					
				<95%	0					
30		La solución de seguridad antivirus cuyo resultado promedio de las evaluaciones realizadas en el año 2021 (de: febrero, junio y agosto) por AV TEST dirigidas a software antivirus en Sistemas Operativos Windows para empresas, respecto a las 3 categorías (protección, rendimiento y usabilidad), alcanzó una puntuación mayor al 95%.	5	>99%	5	3	5	5	4	3
				>98% y <99%	4					
				>97% y <98%	3					
				>96% y <97%	2					
				>95% y <96%	1					
				<95%	0					

[1] No se consideró los resultados de los meses de octubre y diciembre del 2019, ya que dicho producto no aparecía en las evaluaciones dichos meses.

N°	Atributos	Descripción	Puntaje Máximo	Criterios de calificación	Puntaje	ESET	FSECURE	KASPERSKY	MCAFEE	SOPHOS
		Sub Total	**84**			**63**	**67**	**82**	**72**	**54**
ATRIBUTOS DE USO										
31	EFICACIA	Detecta y brinda protección contra amenazas: antes, durante y después de su ejecución.	2	Todas:	2	2	2	2	2	2
				Algunas:	1					
32		Tiene la capacidad de remediar cualquier cambio realizado en los procesos del equipo (causado por algún tipo de infección o amenaza) a su estado de correcto funcionamiento.	2	Si:	2	2	2	2	2	2
				No:	0					
33		Permite realizar escaneados que incluya limpieza de las amenazas: en tiempo real, programado y manual.	2	Todas:	2	2	2	2	2	2
				Algunas:	1					
34		La solución de seguridad antivirus debe permitir realizar un análisis forense de lo ocurrido en los equipos, permitiendo realizar una correlación de eventos que brinde visibilidad detallada de las amenazas presentadas y tener la capacidad de tomar acción como bloqueo de la nueva amenaza detectada, identificar otros equipos con comportamientos similares y aislar los equipos con dichos comportamientos.	2	Todas:	2	1	2	2	2	1
				Algunas:	1					
35	PRODUCTIVIDAD	La consola de administración centralizada EPP debe desplegar actualizaciones compactas e incrementales que eviten la generación de archivos de gran tamaño, evitando que impacte de manera negativa los recursos como ancho de banda y previniendo saturación de la red.	2	Si:	2	2	2	2	2	2
				No:	0					
36		La consola de administración centralizada del componente EPP debe desplegar las actualizaciones a sus clientes de forma automática y de manera más óptima en relación a seguridad y performance.	2	Si:	2	2	2	2	2	2
				No:	0					
37	SEGURIDAD	Evitar que procesos, servicios, archivos o archivos de registro sean detenidos, deshabilitados, eliminados o modificados	2	Todas:	2	2	2	2	2	2
				Algunas:	1					

N°	Atributos	Descripción	Puntaje Máximo	Criterios de calificación	Puntaje	ESET	FSECURE	KASPERSKY	MCAFEE	SOPHOS
		por cualquier tipo de amenaza.								
38		La solución de seguridad antivirus, así como sus diversos componentes deben encontrarse protegido con contraseña para evitar la desinstalación o cambios en la configuración por usuarios no autorizados.	2	Si:	2	2	2	2	2	2
				No:	0					
		Sub Total	**16**			**15**	**16**	**16**	**16**	**15**
		TOTAL	**100**			**78**	**83**	**98**	**88**	**69**

ANEXO 02

Costos Referenciales de licencia por 3 años

Solución de antivirus	Costo de licencia
ESET	S/ 400.00
FSECURE *	S/ 247.80
KASPERSKY	S/ 514.48
MCAFEE	S/ 400.00
SOPHOS *	S/ 259.60

Costos obtenidos en base a cotizaciones referenciales para 1 licencia

* Costos a los que se agregó el 18% de IGV.

Valoración técnico económica					
Solución de antivirus	**Proporción respecto al costo**	**Proporción respecto al beneficio**	**Peso del costo**	**Peso del beneficio**	**Beneficio/ Costo**
ESET	0.62	0.78	0.1	0.9	76.40%
FSECURE	1.00	0.83	0.1	0.9	84.70%
KASPERSKY	0.48	0.98	0.1	0.9	93.02%
MCAFEE	0.62	0.88	0.1	0.9	85.40%
SOPHOS	0.95	0.69	0.1	0.9	71.65%

Análisis Costo-Beneficio			
Solución de antivirus	**Costo de licencias**	**Beneficio**	**Beneficio/Costo**
ESET	S/ 400.00	78	76%
FSECURE	S/ 247.80	83	85%
KASPERSKY	S/ 514.48	98	93%
MCAFEE	S/ 400.00	88	85%
SOPHOS	S/ 259.60	69	72%

Cotizaciones referenciales

ESET

miércoles 29/09/2021 19:12

Richard Concha <rconcha@bafing.com>

RE: Solicitud de cotización referencial-Solución Antivirus ESET

Para JACKELINE JOHANA MELGAREJO REYES

Mensaje ESET.pdf (3 MB)

Estimada Jackeline;
Adjunta la información y valores referenciales de la tecnología **ESET Protect Enterprise** (EEP – EDR – Sandbox).

Ítem	Cant.	Descripción	Precio Unit. S/	Precio Total S/
1	4000	**ESET Protect Enterprise** o Incluye 3-years de ESET Software Business Support.	400.00	1'600,000.00

Los precios están expresados en Soles
Los precios incluyen el 18% del IGV.

Agradeceré confirmar la recepción del presente.

Saludos.

Richard Concha
Gerente Comercial – División de Ciberseguridad
T: (511) 225 9900 * 111 | 996257936
D: Av. Del Parque Sur 560,
San Borja, Lima 15036, Perú
rconcha@bafing.com | www.bafing.com
Expertos en soluciones especializadas de Ciberseguridad, e-Health y Smart Buildings

FSECURE

Innovare Cyberseguridad

Presupuesto
Ref. : PR2110-1226
Ref. cliente : IIF-SECURE CLIENT+EDR 3 Y
Fecha : 16/10/2021
Fecha fin de validez : 15/11/2021
Código cliente : CU1803-0063

Emisor:

INNOVARE E-BUSINESS s.a.c.
AV. JOSE FAUSTINO SANCHEZ CARRION Nº 615
15076 JESUS MARIA

Teléfono: +51 341 8500
Correo: LICITACIONES@INNOVARE.PE
Web: WWW.INNOVARE.PE

Enviar a:

MINISTERIO DE EDUCACION
Ingeniero JACKELINE JOHANA MEGAREJO REYES
CAL.DEL COMERCIO NRO. 193
15034 San Borja
CIF intra.: 20131370998

Importes visualizados en Soles

Descripción	IGV	P.U.	Cant.	Total (Base imp).
F-SECURE ENDPOINT PREMIUM PARA ESTACIONES - ONPREMISE 3AÑOS INCLUYE: [CONSOLA ONPREMISE] > Doble motor antimalware > Antiransomware, Heurística Avanzada, Inteligencia Artificial > Tecnología DataGuard que mejora la protección antiransomware > HIPS, Detección de Vulnerabilidades y Prevención de Explotaciones > Control de Aplicaciones completo con centro de control que permite implementar IoC (Indicadores de Compromiso) para la generación de políticas de seguridad. > Control de Dispositivos completo > Control de Navegación web > Protección de Navegación Web > Gestión de Firewall Avanzado > Gestión de Vulnerabilidades con Aplicación de Parches Multifabricante > Soporte para repositorios en Windows y Linux > Sistema de Aislamiento de Equipos > SANDBOX en la nube con F-Secure Cloud basado en el proyecto BlackFin ganador del Premio a la Excelencia en Inteligencia Artificial 2021 > Permite detectar y bloquear malware nuevo y desconocido en 5 minutos o menos > Integración con Sistemas SIEM, SOAR, SOC https://www.f-secure.com/en/about-us/research/project-blackfin	18%	60.00	4000	240,000.00
F-SECURE ENDPOINT DETECTION AND RESPONSE PARA ESTACIONES - CLOUD 3AÑOS INCLUYE: [CONSOLA EN LA NUBE] > Brinda visibilidad instantánea del estado de la seguridad IT de la empresa > Detecta ataques rápidamente y responde en base a guías expertas > Permite elevar casos a F-Secure para ser revisados por especialistas de la marca. > Tecnología SandBox Broad Context Detection > Buscador de Eventos para la búsqueda de amenazas > Respuestas automatizadas > Análisis de Causa Raíz > Integración con la Técnicas y Tácticas de Ataque de Mitre Att&ck > Visualización de Indicadores de Compromiso > Aislamiento de Equipos > Inventario de Aplicaciones	18%	150.00	4000	600,000.00

KASPERSKY

Adistec

Quote

Adistec Peru S.A.C.
Adistec Peru S.A.C.
Av.Victor Andres Belaunde # 181
Ofic.602-B
San Isidro Lima Lima 27

Date	14/7/2021
Quote #	PE150928
Expires	30/7/2021
Sales Rep	Lorena Gonzales

Señores:

Ministerio de Educación

Presente. -

Atte.: Jorge Trujillo

Estimados Señores:

Tengo el agrado de dirigirme a usted, en atención a la Solicitud de Cotización para el "SERVICIO DE ADQUISICIÓN DE ANTIVIRUS" a fin de remitirle mi oferta técnico - económica conforme a los términos de referencia y/o especificaciones técnicas remitidas.

ITEM	DESCRIPCION	Cantidad	Precio Unitario S/	Precio Total S/
01	**Kaspersky Endpoint Security for Business - Advanced Latin America Edition. 5000 + Node 3 year Base License**	5,000.00	174.64	873,200.00
02	**Kaspersky Endpoint Detection and Response Advanced Latin America Edition. 5000 + Node 3 year Base License**	5,000.00	339.84	1,699,200.00
	TOTAL GENERAL S/			**2,572,400.00**

CONDICIONES COMERCIALES:

- Precios expresados en Soles e incluye IGV.
- Validez de la oferta: 30 de Julio.

MCAFEE

miércoles 29/09/2021 19:20

Richard Concha <rconcha@bafing.com>

RE: Solicitud de cotización referencial-Solución Antivirus McAfee

Para JACKELINE JOHANA MELGAREJO REYES

Mensaje | McAfee MV6.pdf (867 KB) | ds-advanced-threat-defense.pdf (551 KB)

Estimada Jackeline:
Adjunta la información y valores referenciales de la tecnología **McAfee MVISION Protect Plus EDR for Endpoint + Advanced Threat Defense** (EEP – EDR – Sandbox).

Ítem	Cant.	Descripción	Precio Unit. S/	Precio Total S/
1	4000	**McAfee MVISION Protect Plus EDR for Endpoint & Advanced Threat Defense** o Incluye 3-years de McAfee Software Business Support.	400.00	**1'600,000.00**

Los precios están expresados en Soles
Los precios incluyen el 18% del IGV.

Agradeceré confirmar la recepción del presente.

Saludos.

Richard Concha
Gerente Comercial – División de Ciberseguridad
T: (511) 225 9900 * 111 | 996257936
D: Av. Del Parque Sur 560,
San Borja, Lima 15036, Perú
rconcha@bafing.com | www.bafing.com
Expertos en soluciones especializadas de Ciberseguridad, e-Health y Smart Buildings

SOPHOS

Innovare Cyberseguridad

Presupuesto
Ref. : PR2110-1224
Ref. cliente : SOPHOS CIX ADV 3Y
Fecha : 16/10/2021
Fecha fin de validez : 15/11/2021
Código cliente : CU1803-0063

Emisor:

INNOVARE E-BUSINESS s.a.c.
AV. JOSE FAUSTINO SANCHEZ CARRION Nº 615
15076 JESUS MARIA

Teléfono: +51 341 8500
Correo: LICITACIONES@INNOVARE.PE
Web: WWW.INNOVARE.PE

Enviar a:

MINISTERIO DE EDUCACION
Ingeniero JACKELINE JOHANA MEGAREJO REYES
CAL.DEL COMERCIO NRO. 193
15034 San Borja
CIF intra.: 20131370998

Importes visualizados en Soles

Descripción	IGV	P.U.	Cant.	Total (Base imp).
SOPHOS INTERCEPTX AVANZADO + EDR - CLOUD 1AÑO INCLUYE: [CARACTERÍSTICAS ENDPOINT] > Motor antimalware > Antiransomware, Heurística Avanzada, Deep Learning > Tecnología CryptoGuard que mejora la protección antiransomware > HIPS, Detección de Vulnerabilidades y Prevención de Explotaciones > Control de Aplicaciones administrador por el fabricante > Control de Dispositivos > Control de Navegación web > Protección de Navegación Web > Gestión de Firewall Avanzado > Soporte para repositorios en Windows > SANDBOX en la nube con Sophos Cloud basado en SandStorm > Integración con Sistemas SIEM [CARACTERÍSTICAS EDR] > Brinda visibilidad instantánea del estado de la seguridad IT de la empresa > Detecta ataques rápidamente y responde en base a guías expertas > Buscador de Eventos para la búsqueda de amenazas > Análisis de Causa Raíz > Analisis de archivos sospechosos > Visualización de Indicadores de Compromiso > Sistema OSQuery para realizar consultas remotas en los equipos > Acceso vía terminal a los equipos para casos de soporte	18%	220.00	4000	880,000.00