INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE ANTIVIRUS CORPORATIVO

INFORME N° 293-2018-MED-SPE-OTIC

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

2. **RESPONSABLE DE LA EVALUACIÓN**
   Jackeline Melgarejo Reyes
   Jose Choque Herrera

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

4. **FECHA**
   Febrero del 2018

5. **JUSTIFICACIÓN**
   El Ministerio de Educación requiere contar con una solución que permite 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 todo tipo de amenazas ya sea de virus, spyware, bootent, malware y variantes de los mismos, brindando protección ante todo tipo de amenazas tanto conocidas como desconocidas.
   Debido a 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, el mismo 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.
   Por ello es crucial contar con una solución de antivirus para el Ministerio de Educación, brindando protección a todas sus sedes desconcentradas, ubicadas en el ámbito de Lima Metropolitana.
   Por lo expuesto y 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 del software Antivirus Corporativo.

6. **ALTERNATIVAS**
   Tomando en consideración las necesidades y requerimientos del Ministerio de Educación, tomando en cuenta los nuevos esquemas relacionados con protección ante amenazas no solo conocidas, sino también desconocidas, se ha buscado alternativas de software antivirus en el mercado local que cumplan dichas necesidades y cuenten con soporte técnico local.
   Debido e ello, la herramienta de software 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.

Por ello, se ha establecido parámetros mínimos que permitan fortalecer la seguridad en las TI obteniendo disponibilidad, integridad y confidencialidad, como factores que conllevan a una mejor evaluación. 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, 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:

- TREND MICRO.
- MCAFEE.
- KASPERSKY.

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 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 aprobado 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	60
2	EFICIENCIA	8
3	CAPACIDAD DE MANTENIMIENTO	2
4	PORTABILIDAD	4
5	FIABILIDAD	10
ATRIBUTOS DE USO		
1	EFICACIA	12
2	PRODUCTIVIDAD	2
3	SEGURIDAD	2
	TOTAL	**100**

MINISTERIO DE EDUCACIÓN Unidad de Infraestructura Tecnológica Área de Comunicaciones Y Seg. Lógica OTIC - UIT V°B°

MINISTERIO DE EDUCACIÓN UIT OTIC

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.

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 normativa vigente.

9. CONCLUSIONES

En base al análisis realizado, se evidencia que los tres productos evaluados, TREND MICRO, MCAFEE y KASPERSKY cumplen con las características técnicas mínimas solicitas para la protección que corresponde al software 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.

10. FIRMAS

Jackeline Melgarejo Reyes
Especialista del Área de Comunicaciones y Seguridad Lógica UIT-OTIC
Ministerio de Educación

MINISTERIO DE EDUCACIÓN Unidad de Infraestructura Tecnológica V°B° Área de Comunicaciones y Seg. Lógica OTIC - UIT

Jose Choque Herrera
Coordinador del Área de Comunicaciones y Seguridad Lógica UIT-OTIC
Ministerio de Educación

MINISTERIO DE EDUCACIÓN UIT

Johny Meregildo Ramos
Jefe de la Unidad de Infraestructura Tecnológica de la Oficina de Tecnologías de la Información y Comunicación
Ministerio de Educación

Alberto Carlos Pajuelo Huaman
Jefe de la Oficina de Tecnologías de la Información y Comunicación
Ministerio de Educación

ANEXO 01

CARACTERÍSTICAS TÉCNICAS DE SOFTWARE ANTIVIRUS CORPORATIVO

N°	Atributos	Descripción	Puntaje Máximo	TREND MICRO	MCAFEE	KASPERSKY
ATRIBUTOS INTERNOS Y EXTERNOS						
1	FUNCIONALIDAD	Es una solución basada 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.	4	4	4	4
		Brinda protección en base a una nube dedicada a proteger proactivamente todo tipo amenazas, que incluye: a) Amenazas conocidas y b) Amenazas desconocidas.	4	4	4	4
		Protección contra todo tipo de amenazas como: a) Virus, b) Gusanos, c) Troyanos, d) Keyloggers, e) Dialers, f) Adware, g) Spyware, h) Hacktools, i) Rootkits, j) Bots, k) Phishing, l) Herramientas de control remoto, m) Ransomware, n) Programas o software maliciosos, o) Todo tipo de malware existente y nuevas variantes.	4	4	4	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 al equipo.	2	2	2	2
		Permite realizar escaneados que incluya limpieza de las amenazas: a) En tiempo real, b) Programado, c) Manual.	4	4	4	4
		Defiende contra amenazas aun cuando estas tengan mecanismos para eludir las tecnologías de detección como: a) Código malicioso empaquetado, b) Ofuscación de código, c) Polimorfismo, d) Cifrado, e) Vulnerabilidades, f) Omisión de emuladores, g) Otras nuevas que puedan surgir así como la combinación de las mismas.	4	4	4	4
		Tiene la capacidad de defender los sistemas contra amenazas que causen buffer overflows (desbordamientos de buffer) y ataques combinados.	1	1	1	1
		Detectar, analizar y eliminar, de forma automática y en tiempo real amenazas que se encuentren en: a) Programas maliciosos que generen procesos que se ejecutan en la memoria principal (RAM), b) Archivos ejecutables, c) Aplicaciones, d) Archivos comprimidos, de forma automática, e) Archivos recibidos a través de software de comunicación instantánea, f) Archivos ocultos, g) Archivos en ejecución.	1	1	1	1
		Monitorea y evita que un programa sospechoso o amenaza realice las siguientes acciones: a) Incrusten plug-ins en navegadores, b) Instale nuevos servicios, c) Modifique archivos de sistema, d) Instale servicios o programas para iniciarse al arrancar la estación de trabajo.	1	1	1	1

MINISTERIO DE EDUCACIÓN Unidad de Infraestructura Tecnológica Área de Comunicaciones y Data Logística OTIC - UIT - V°B°

MINISTERIO DE EDUCACIÓN UIT OTIC

CARACTERÍSTICAS TÉCNICAS DE SOFTWARE ANTIVIRUS CORPORATIVO

N°	Atributos	Descripción	Puntaje Máximo	TREND MICRO	MCAFEE	KASPERSKY
		Permite la protección ante amenazas existentes en: a) Las diferentes particiones de disco del equipo, b) Unidades de red, c) Medios extraíbles tales como dispositivos de almacenamiento USB, d) CD/DVD.	1	1	1	1
		Debe evitar todo tipo de infección provocada por la ejecución automática de cualquier tipo de archivo proveniente de un dispositivos tipo USB (memoria/disco duro) al momento de ser conectado en la estación de trabajo, de forma automática y sin requerir un escaneo previo.	1	1	1	1
		Permite el control sobre los archivos y/o unidades que deben ser analizados cuando se realicen escaneos manuales o programados, con la capacidad de excluir o incluir particiones, unidades de red, carpetas, archivos, medios extraíbles de los equipos.	1	1	1	1
		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.	1	1	1	1
		Poseer tecnología de prevención y protección contra "exploit", independientemente del medio por el que intente infectar al equipo.	4	4	4	4
		Tiene la capacidad de crear discos de rescate que permitan escanear particiones antes que cargue el sistema operativo o en su defecto debe proteger y analizar los sectores de arranque del equipo.	1	1	1	1
		Notifica al usuario cuando exista algún riesgo de infección detectada.	1	1	1	1
		Permite generar paquetes de instalación personalizados que tengan la licencia y últimas actualizaciones.	1	1	1	1
		Firewall: Incluye firewall del mismo fabricante, administrado desde la consola de administración, permitiendo bloquear y autorizar puertos específicos, mediante la creación de reglas por: dirección IP, dirección MAC y/o puerto de origen; y dirección IP, dirección MAC y/o puerto destino.	2	2	2	2
		Control de aplicaciones: Permite autorizar y bloquear aplicaciones en base a listas blancas o negras que contienen aplicaciones recomendadas y no recomendadas para uso, en base a criterios de seguridad del propio fabricante del producto, así como personalizar el uso o bloqueo de dichas aplicaciones, creando exclusiones a los criterios establecidos por el fabricante.	2	2	2	2
		Protección de vulnerabilidades: Cuenta con tecnologías que permita mitigar el riesgo y brindar protección ante la explotación de vulnerabilidades en sistemas operativos y aplicaciones que tengan los clientes.	2	2	2	2

CARACTERÍSTICAS TÉCNICAS DE SOFTWARE ANTIVIRUS CORPORATIVO

N°	Atributos	Descripción	Puntaje Máximo	TREND MICRO	MCAFEE	KASPERSKY
		Control Web: Permite navegar a internet de forma segura, usando heurística y otras técnicas de protección solicitadas, bloqueando de manera proactiva: a) Cualquier descarga dañina, b) Cualquier amenaza en el código HTML, c) Código malicioso, d) Software espía, e) Enlaces ocultos a otros sitios web dañinos que infecten las estaciones de trabajo. Incluye protección web a páginas HTTPS. Protección brindada incluso antes que el navegador comience a descargar el contenido de la web. Muestra mensajes de advertencia sobre la navegación a sitios maliciosos a los que buscan 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.	2	2	2	2
		Control de dispositivos: Permite el control (bloqueo y/o habilitación) de dispositivos como mínimo 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.	2	2	2	2
		Reportes: Permite crear reportes personalizados, programadas, con envío a correo electrónico a cuentas específicas. Estos deben ser exportados como mínimo en los formatos: html y pdf, adicionalmente por csv o xml. Permite envío de alertas de fallas o infecciones. Permite visualizar el detalle de los equipos como nombre del equipo, ip, último usuario conectado, incluya fecha y hora. Para amenazas que no fueron bloqueadas, deben mostrarse el mapeo de los equipos afectados, los cambios que realizaron en los equipos y la afección que esto causa. Los reportes personalizados deben permitir como mínimo crear: a) Reportes de amenazas bloqueadas, b) Reportes de amenazas no bloqueadas, c) Reportes equipos infectados, d) Reportes de equipos con errores/tipo de errores, e) Reportes de equipos que no actualizan, f) Reportes de sitios web bloqueados, g) Reportes de aplicaciones bloqueadas.	2	2	2	2
		La solución de antivirus debe ser administrada y configurada de forma remota desde una consola de antivirus centralizada, siendo ambos de la misma marca. En caso de existir más de una consola de administración que complemente las características solicitadas, tanto la solución de antivirus como las consolas de administración deben ser de la misma marca. Además, las consolas deben encontrarse sincronizadas compartiendo la información de seguridad que permitan brindar la protección a	1	1	1	1

MINISTERIO DE EDUCACIÓN Unidad de Infraestructura Tecnológica VoBo Área de Comunicaciones y Seg Lógica OTIC UIT

MINISTERIO DE EDUCACIÓN UIT OTIC

CARACTERÍSTICAS TÉCNICAS DE SOFTWARE ANTIVIRUS CORPORATIVO

02

N°	Atributos	Descripción	Puntaje Máximo	TREND MICRO	MCAFEE	KASPERSKY
		todos los equipos que se encuentran bajo su administración.				
		La consola de administración debe contar con repositorios distribuidos (para las sedes desconcentradas, existiendo dos escenarios: sedes que se encuentran en la red de la Institución y sedes que actualizan por internet), las mismas que permitirán como mínimo realizar la actualización de la solución antivirus en las estaciones de trabajo que están bajo su gestión.	1	1	1	1
		La consola de administración debe permitir: a) Monitorear el total de las estaciones de trabajo que tiene a su cargo, b) La creación y ejecución de tareas o políticas para grupos y/o equipos específicos, c) Detectar antivirus de terceros instalados en las estaciones de trabajo y proceder con la desinstalación automática antes de instalar el antivirus ofertado, d) Tomar acción en caso se detecte una estación esté infectada, e) Crear políticas de denegación de escritura centralizada para evitar epidemias, f) La creación de usuarios con diferentes roles de administración, g) Almacenar el histórico de eventos de cada estación administrada, h) Generar reportes gráficos y personalizados, i) La instalación y desinstalación del cliente de manera "Silenciosa", desatendida y remota desde la consola de administración, con la capacidad de retrasar/suprimir la necesidad del re-inicio, j) El envío de notificaciones de SMTP o SNMP, de los eventos más importantes de la solución endpoint, k) Visualizar de manera rápida y sencilla el estado del antivirus en los equipos de cómputo (activo e inactivo), acción realizada ante las nuevas amenazas y estadísticas más resaltantes.	4	4	4	4
		La consola de administración debe ser capaz de: a) escanear la red por directorio activo, red IP o dominios en busca de nuevos equipos agregados a la red, b) notificar los intentos de infección de amenazas, de acuerdo a parámetros definidos por el administrador de la solución, que incluya los resultados ocurridos en los equipos, c) bloquear cualquier cambio que el usuario requiera realizar sobre la configuración y/o deshabilitación del antivirus en el equipo. Esto debe encontrarse protegido con contraseña, d) realizar configuraciones transparentes para el usuario, las mismas que deben ser registradas en los eventos.	4	4	4	4
		La consola de administración debe proporcionar la siguiente información de los equipos: nombre del equipo, descripción, sistema operativo, dominio al que pertenece, dirección IP, último usuario conectado, fecha y hora de la última actualización, eventos de amenazas y eventos de error.	1	1	1	1

CARACTERÍSTICAS TÉCNICAS DE SOFTWARE ANTIVIRUS CORPORATIVO

N°	Atributos	Descripción	Puntaje Máximo	TREND MICRO	MCAFEE	KASPERSKY
		La consola de antivirus debe funcionar con base de datos que almacenará la información relacionada a los eventos de la plataforma de antivirus en tiempo real. Debe incluir el motor de base de datos con el que trabaja.	1	1	1	1
2	EFICIENCIA	Detecta, detiene, bloquea y evita la instalación, propagación e infección de todo tipo de amenazas.	4	4	4	4
		Brinda protección aun cuando esta comprometa al sistema operativo y/o aplicación, incluso cuando no existan parches o actualizaciones que cubran dicha vulnerabilidad.	4	4	4	4
3	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.	1	1	1	1
		La consola de antivirus debe tener la capacidad de conectarse automáticamente a Internet y descargar las actualizaciones necesarias para todos los productos activados. Dicha conexión deberá poder configurarse por minuto, hora, día o mes.	1	1	1	1
4	PORTABILIDAD	Compatible con estaciones de trabajo: Microsoft Windows 7, 8, 8.1, 10, con soporte para 32 y 64 bits.	1	1	1	1
		La consola centralizada debe tener la capacidad de instalarse en plataformas Windows Server 2012, 2012 R2 y superior. Los repositorios distribuidos deben tener la capacidad de instalarse en plataformas Windows Clientes (Vista, 7, 8, 8.1, 10).	1	1	1	1
		La consola de antivirus debe tener la capacidad de configurar políticas móviles para que cuando un equipo esté fuera de la red institucional, pueda actualizarse vía internet.	2	2	2	2
5	FIABILIDAD	Se encuentra como líder en el cuadrante mágico de Gartner para Endpoint en los años 2016 y 2017 de forma consecutiva.	2	2	1	1
		Para todas las evaluaciones de software antivirus para empresas realizadas a Sistemas operativos Windows por AV TEST en los años 2016 y 2017, con respecto al test de protección en tiempo real, alcanzaron un nivel de protección mayor o igual al 99.4%.	2	1	1	1
		Para todas las evaluaciones de software antivirus para empresas realizadas a Sistemas operativos Windows por AV TEST en los años 2016 y 2017, con respecto al test de detección de malware más extendidos y frecuentes, alcanzaron un nivel de protección mayor o igual al 99.9%.	2	1	1	2
		Para todas las evaluaciones realizadas por AV COMPARATIVES en los años 2016 y 2017, con respecto al test "Real-World", alcanzaron un ratio de protección mayor al 99.41%.	2	2	1	2

MINISTERIO DE EDUCACIÓN Unidad de Infraestructura Tecnológica VºBº Área de Comunicaciones y Seg. Lógica OTIC - UIT

MINISTERIO DE EDUCACIÓN UIT OTIC

CARACTERÍSTICAS TÉCNICAS DE SOFTWARE ANTIVIRUS CORPORATIVO

N°	Atributos	Descripción	Puntaje Máximo	TREND MICRO	MCAFEE	KASPERSKY
		Para todas las evaluaciones realizadas por AV COMPARATIVES en el año 2017, con respecto al test "Malware Protection", alcanzaron un ratio de protección mayor o igual al 99.91%.	2	2	1	2
		Sub Total	**84**	**82**	**79**	**82**
ATRIBUTOS DE USO						
1	EFICACIA	Detecta y brinda protección contra amenazas: a) Antes de su ejecución (pre-execution), b) En ejecución (on-execution), c) Después de su ejecución (post-execution).	4	4	4	4
		Tiene la capacidad de remediar cualquier cambio realizado en los procesos del equipo (causado por algún tipo de infección o amenza) a su estado de correcto funcionamiento.	4	4	4	4
		La solución de 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.	4	4	4	4
2	PRODUCTIVIDAD	La consola de administración 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.	1	1	1	1
		La consola de administración debe desplegar las actualizaciones a sus clientes de forma automática y de la manera más óptima en relación a seguridad y performance.	1	1	1	1
3	SEGURIDAD	Evitar que procesos, servicios, archivos o archivos de registro sean detenidos, deshabilitados, eliminados o modificados por cualquier tipo de amenaza.	1	1	1	1
		El antivirus cuenta con protección para evitar: a) La desinstalación y cambios en la configuración por parte de usuarios no autorizados, b) La deshabilitación de los servicios relacionados con el mismo antivirus aun cuando el usuario tenga permisos de administrador en el equipo.	1	1	1	1
		Sub Total	**16**	**16**	**16**	**16**
		TOTAL	**100**	**98**	**95**	**98**

MINISTERIO DE EDUCACIÓN Unidad de Infraestructura Tecnológica Área de Comunicaciones Y Seg. Lógica VoBo OTIC - UIT

MINISTERIO DE EDUCACIÓN UIT OTIC

ANEXO 02

Costos Referenciales de licencia por 3 años

Software	Costo de Licencia
TREND MICRO	S/. 3,164,997.15
MCAFEE	S/. 1,303,193.72
KASPERSKY	S/. 355,793.60

* Costos referenciales para 4000 licencias.

** Tipo de cambio de dolares a soles: 3.26.

*** Costos incluyen IGV.

Análisis Costo-Beneficio

Software	Costo Total	Beneficio	Beneficio/Costo
TREND MICRO	S/. 3,164,997.15	98	0.89
MCAFEE	S/. 1,303,193.72	95	0.88
KASPERSKY	S/. 355,793.60	98	0.98

MINISTERIO DE EDUCACIÓN Unidad de Infraestructura Tecnológica Área de Comunicaciones Y Seg Lógica VºBº OTIC - UIT

MINISTERIO DE EDUCACIÓN UIT OTIC