"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Fortalecimiento de la Soberanía Nacional"

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE N° 001-2024-MIDI/PNPAIS-UTI-MACP SOFTWARE ANTIVIRUS

1. NOMBRE DEL ÁREA

Unidad de Tecnologías de la Información - UTI

2. RESPONSABLE DE LA EVALUACIÓN

Nombre: Jorge Luis Tavara Vallejos
Cargo: Ejecutivo de la Unidad de Tecnologías de la Información

Nombre: Martin Artemio Cruz Palacios
Cargo: Analista de Soporte Operacional y Servicios TI

3. FECHA

02 de abril de 2024

4. JUSTIFICACIÓN

El Programa Nacional "Plataformas de Acción para la Inclusión Social – PAIS" requiere contar con una solución que garantice la adecuada protección de la información almacenada en los equipos y de los sistemas informáticos de la institución, de ser modificada, borrada o afectada por programas no deseados, como virus informáticos, troyanos, spyware y nuevas variantes de estos.

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.

Actualmente el Programa Nacional PAIS cuenta con un software ANTIVIRUS, que incluye licencias hasta el 21 de noviembre del 2024. Por ello, es crucial contar con una solución de protección antivirus para los equipos informáticos (EndPoint) debido al nivel de tráfico de información en la red interna (LAN) y extendida (WAN).

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

5. ALTERNATIVAS DE EVALUACIÓN:

Considerando los requerimientos del Programa Nacional PAIS, se han buscado diversos softwares en el medio local que cumplan con los requerimientos.

Es por ello, que la herramienta de software que sea seleccionada debe contener como mínimo las funcionalidades que permitan mayor protección a la información que se maneja en el Programa Nacional PAIS.

Por lo mencionado, se ha establecido parámetros en base a la experiencia y a las mejores prácticas en el Programa Nacional PAIS, estableciendo criterios que fortalezcan la seguridad en las tecnologías de información obteniendo disponibilidad, integridad y confidencialidad, como factores que conlleven a una mejor evaluación.

En base a estas premisas y la información encontrada se está evaluando las siguientes soluciones:

- ESET NOD
- KASPERSKY
- SOPHOS

Para la determinación de estas soluciones, así como la evaluación técnica y para la elaboración de los TDR, se ha tomado como referencia:

Información disponible en las páginas web de cada uno de los productos antivirus (ver Anexo 1).

6. ANÁLISIS COMPARATIVO TÉCNICO.

El análisis comparativo técnico está basado en la metodología establecida en la "Guía técnica sobre evaluación de software en la administración pública", aprobada por la Resolución Ministerial N° 139-2004-PCM, tal como se exige en el reglamento de Ley N° 28612.

6.1. Propósito de Evaluación

Validar que las alternativas seleccionadas sean las más convenientes para el Programa Nacional PAIS

6.2. Identificar el Tipo de Producto

Software antivirus para equipos de cómputo de escritorio, laptops y servidores.

6.3. Identificación del Modelo de Calidad

Para la evaluación técnica del Software antivirus se aplicará el modelo de calidad descrito en la parte 1 de la Guía de evaluación de software aprobada por R.M. Nº 139-2014-PCM y la Ley Nº 28612 – "Ley que norma el uso, adquisición y adecuación del software en la administración pública".

6.4. Selección de Métricas

La selección de métricas se obtuvo a partir de los atributos especificados en el modelo de calidad, tal como se muestra a continuación:

N°	ATRIBUTOS	Puntaje Máximo
ATRIBUTOS INTERNOS Y EXTERNO		
1	FUNCIONALIDAD	61
2	EFICIENCIA	8
3	CAPACIDAD DE MANTENIMIENTO	2
4	PORTABILIDAD	7
ATRIBUTOS DE USO		
1	EFICACIA	16
2	PRODUCTIVIDAD	2
3	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 que se muestran en el siguiente punto.

6.5. Análisis Comparativo Técnico/Funcional

N°	Atributos	Descripción	Puntaje Máximo	Eset	Kasper Sky	So Phos
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	3
		Protección contra todo tipo de amenazas como: virus, gusanos, troyanos, keyloggers, dialers, adware, spyware, hacktools, rootkits, bots, phishing, herramientas de control remoto, ransomware, programas o software maliciosos, y 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/servidor.	**4**	4	4	4

N°	Atributos	Descripción	Puntaje Máximo	Eset	Kasper Sky	So Phos
		Permite realizar escaneados que incluya limpieza de las amenazas: en tiempo real, programado y manual.	**2**	2	2	2
		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) 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.	**2**	2	2	2
		Monitorea y evita que un programa sospechoso o amenaza realice las siguientes acciones: a) Se incruste 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
		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.	**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 al equipo/servidor, 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	**2**	2	2	2
		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/segmento de red y puerto de origen; y dirección IP/segmento de red y 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,	**2**	1	1	1

N°	Atributos	Descripción	Puntaje Máximo	Eset	Kasper Sky	So Phos
		creando exclusiones a los criterios establecidos por el fabricante				
		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 los servidores. 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. Permite la configuración del control de dispositivos para: bloqueo, solo lectura, control total. Dicha configuración puede realizarse por equipo/servidor o por usuario.	**2**	2	2	2
		Protección de vulnerabilidades: Cuenta con tecnologías que permiten mitigar el riesgo y brindar protección ante la explotación de vulnerabilidades en sistemas operativos y aplicaciones que tengan los equipos/servidores.	**2**	2	2	2
		Reportes: Permite crear reportes personalizados, programados, 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, incluyendo 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.	**1**	1	1	1
		La consola de administración local o en nube 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 o directivas para grupos y/o equipos específicos, c) Tomar acción en caso se detecte una estación esté infectada, d) Crear políticas de denegación de escritura centralizada para evitar epidemias, e) La creación de usuarios con diferentes roles de administración, f) Almacenar el histórico de eventos de cada estación administrada, g) Generar reportes gráficos y personalizados, h) Visualizar de manera rápida y sencilla el estado del antivirus en los equipos/servidores (activo e inactivo), acción realizada ante las nuevas amenazas y estadísticas más resaltantes, h) bloquear cualquier cambio que el usuario requiera realizar sobre la configuración y/o deshabilitación del antivirus en el equipo ya que debe encontrarse protegido con contraseña, i) realizar configuraciones transparentes para el usuario, las mismas que deben ser registradas en los eventos.	**4**	3	3	3

N°	Atributos	Descripción	Puntaje Máximo	Eset	Kasper Sky	So Phos
		Adicionalmente, la consola de administración local o de nube, debe permitir: a) Detectar antivirus de terceros instalados en las estaciones de trabajo y proceder con la desinstalación automática antes de instalar el antivirus ofertado, b) 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, c) El envío de notificaciones de SMTP o SNMP, de los eventos más importantes de la solución endpoint, d) escanear la red por directorio activo, red IP o dominios en busca de nuevos equipos agregados a la red, e) 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.	**4**	3	3	3
		La consola de administración debe proporcionar la siguiente información de los equipos/servidores: nombre del equipo, 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
		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. De requerirlo, debe incluir el motor de base de datos con el que trabaja.	**1**	1	1	1
		Detecta, detiene, bloquea y evita la instalación, propagación e infección de todo tipo de amenazas.	**4**	4	4	4
2	**EFICACIA**	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 MANTENI-MIENTO**	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 periodos como: hora o día.	**1**	1	1	1
	PORTABI-LIDAD	Compatible con Sistema Operativo: Microsoft Windows Server 2016 en adelante, tanto para servidores físicos como virtuales.	**2**	2	2	2
		La consola centralizada local debe tener la capacidad de instalarse en plataformas Windows Server 2016 y superior	**1**	1	1	1
		La consola centralizada también debe tener la capacidad de operar en la nube	**4**	3	2	3
SUB-TOTAL			**78**	74	73	73
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 amenaza) a su estado de correcto funcionamiento.	**4**	3	3	3
		La solución de antivirus no debe afectar el performance del equipo/servidor. No debe consumir más del 20% de los recursos de memoria y CPU.	**4**	3	2	2
		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**	3	3	3
2	**PRODUCTI-VIDAD**	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

N°	Atributos	Descripción	Puntaje Máximo	Eset	Kasper Sky	So Phos
		La consola de administración debe desplegar las actualizaciones a sus clientes de forma automática y de la manera óptima en relación con 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	**2**	2	2	2
		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.	**2**	2	2	2
		SUB TOTAL	**22**	19	18	18
		TOTAL	**100**	93	91	91

Considerando que la suma de los puntajes máximos es 100 para la evaluación de alternativas, se considerará la siguiente tabla de aceptación de alternativas.

Rango de puntaje	Descripción
[75-100>	**Altamente Recomendable.** Cumple totalmente con los requerimientos y expectativas.
[50-74>	**Riesgoso.** Cumple parcialmente con los requerimientos, pero no se garantiza su adaptación a sus necesidades.
[0-49>	**No Recomendable.** Software con características inadecuadas.

7. ANÁLISIS COMPARATIVO DE COSTO-BENEFICIO.

Análisis Comparativo Costo – Beneficio Para efectuar el análisis de Costo Beneficio se tiene en cuenta lo expresado en los siguientes cuadros:

VALORACIÓN DE LA CALIDAD DE USO:			
TOTAL = (ATRIBUTOS DE USO + ATRIBUTOS INTERNOS Y EXTERNOS) / 2			
VALORACION	**ESET**	**KASPERSKY**	**SOPHOS**
Total, Métricas de atributos internos y externos	74	73	73
Total, Métricas de atributos de Uso	19	18	18
RESULTADO VALORACION DE LA CALIDAD DE USO	46.5	45.5	45.5

VALORACION DEL COSTO DE LICENCIAMIENTO:

Costo	Puntaje
Alto costo	1
Costo medio	2
Costo bajo	3

Nota: Al costo más bajo se le asigna un puntaje mayor.

VALORACIÓN DE REFERENCIA:

Producto	Precio estimado por 100 suscripciones de licencia anual de usuario (*)	Valoración
ESET	S/11,398.80	3
KASPERSKY	S/12,852.00	1
SOPHOS	S/12,058.80	2

(*) Precios referenciales de la web del fabricante verificado el 07/03/2024, ver anexo 01.

VALORACION DEL COSTO DE HARDWARE NECESARIO PARA SU FUNCIONAMIENTO

Producto:	Resultado:	Valoración
ESET	El costo del hardware para el funcionamiento de ambos softwares es cero Soles (S/. 0.00), ya que no se necesita hardware adicional para la implementación de la solución. La institución cuenta con el hardware necesario.	3
KASPERSKY		3
SOPHOS		3

IMPACTO EN EL CAMBIO DE PLATAFORMA DE GESTIÓN

Producto:	Resultado:	Valoración
ESET	El área de TI si se encuentra familiarizado con el software.	3
KASPERSKY	El área de TI no se encuentra familiarizado con el software.	1
SOPHOS	El área de TI no se encuentra familiarizado con el software.	1

IMPACTO EN EL CAMBIO DE PLATAFORMA PARA LOS USUARIOS

Producto:	Resultado:	Valoración
ESET	El área usuaria si se encuentra familiarizado con el software.	3
KASPERSKY	El área usuaria no se encuentra familiarizado con el software.	1
SOPHOS	El área usuaria no se encuentra familiarizado con el software.	1

VALORACION DEL COSTO TOTAL:

COSTOS	ESET	KASPERSKY	SOPHOS
VALORACION DEL COSTO DE LICENCIAMIENTO	3	1	2
VALORACION DEL COSTO DE HARDWARE NECESARIO PARA SU FUNCIONAMIENTO	3	3	3
VALORACIÓN DEL IMPACTO EN EL CAMBIO DE PLATAFORMA DE GESTIÓN	3	1	1
VALORACIÓN DEL IMPACTO EN EL CAMBIO DE PLATAFORMA PARA LOS USUARIOS	3	1	1
VALORACION COSTO TOTAL	**12**	**6**	**7**

Para determinar la Valoración Total se aplica el siguiente criterio:

VALORACIÓN TOTAL

$$\text{TOTAL} = \frac{\text{METRICA TECNICO FUNCIONAL} + \text{VALORACION DEL COSTO BENEFICIO}}{2}$$

VALORACION	ESET	KASPERSKY	SOPHOS
VALORACIÓN DE LA CALIDAD DE USO	46.5	45.5	45.5
VALORACIÓN DEL COSTO TOTAL	12	6	7
VALORACION TOTAL	29.25	25.75	26.25

8. CONCLUSIONES

En base a la evaluación técnica y de acuerdo con la necesidad funcional que se requiere, se evidencia que, de los tres productos evaluados, el antivirus ESET es recomendable para el Programa Nacional PAIS, ya que obtiene un mayor puntaje en la evaluación realizada. Por lo tanto, se recomienda la adquisición de licencias del producto con mejor puntaje en conformidad al informe de evaluación presentado. Asimismo, permite cumplir con la normatividad vigente, relacionada a la legalidad del software informático.

9. FIRMAS

Nombre	Cargo	Firma
Jorge Luis Tavara Vallejos	Ejecutivo de la Unidad de Tecnologías de la Información	Firmado digitalmente por TAVARA VALLEJOS Jorge Luis FAU 20601993181 soft Motivo: Soy el autor del documento Fecha: 09.04.2024 17:18:42 -05:00
Martin Artemio Cruz Palacios	Analista de Soporte Operacional y Servicios TI	Firmado digitalmente por CRUZ PALACIOS Martin Artemio FAU 20601993181 soft Motivo: Soy el autor del documento Fecha: 03.04.2024 11:58:03 -05:00