

SAT SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DELIMA	LEY 28612 LEY QUE NORMA EL USO, ADQUISICIÓN Y ADECUACIÓN DEL SOFTWARE EN LA ADMINISTRACIÓN PÚBLICA	Fecha: 07.03.2025
	INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE	Página 1 de 4

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE N°001-2025-OTI/SAT

1. NOMBRE DEL OFICINA:

Oficina de Tecnologías de la Información

2. RESPONSABLES DE LA EVALUACIÓN:

Edwin Turín Avila
Cesar Edilberto Terry Ramos

3. CARGO:

Especialista de Gestión de Operaciones de TI II

4. FECHA DE APROBACIÓN

07 de marzo del 2025

5. JUSTIFICACIÓN

Se requiere de una solución que permita proteger los activos de cómputo de la institución incluyendo los sistemas informáticos que podrían verse afectados en la alteración y/o eliminación de manera no autorizada por causa de programas maliciosos conocidos como virus informáticos como troyanos, spyware, malware, ransomware entre otras variantes.

La institución, en relación a la existencia de nuevas amenazas, requiere contar con herramientas cuyas funciones específicas permitan mitigar el riesgo de los softwares con códigos maliciosos (malware) entre otros. Por tal motivo es necesario contar con una solución de software de antivirus con capacidades de prevención, mitigación, detección y recuperación ante amenazas ciberneticas con la finalidad de garantizar una protección a nivel de endpoint en la red de la institución.

El presente informe tiene como finalidad contratar una solución y soporte técnico, para lo cual se realizará la evaluación respectiva.

6. ALTERNATIVAS.

La evaluación técnica del software se ha realizado tomando como referencia productos similares en el mercado con características y requerimientos de instalaciones semejantes y cubran el requerimiento de la institución, considerando como alternativa a las siguientes marcas:

Symantec Protection Suite Enterprise Edition.
Kaspersky Endpoint Detection and Response Optimum.
With Secure Elements Endpoint Protection.

7. ANALISIS COMPARATIVO TÉCNICO

Se analizó aplicando los siguientes criterios.

a. Propósito de la Evaluación:

Encontrar un software que permita satisfacer las necesidades de prevención, mitigación, detección y recuperación ante ataques de malware. El propósito es determinar los atributos o características para el producto final.

b. Identificar el tipo de producto

Software para la protección contra todo tipo de software malicioso.

c. Cuadro comparativo de software:

CUADRO 1 METRICAS: ATRIBUTOS INTERNOS Y EXTERNOS							
Nº	ATRIBUTO	DESCRIPCIÓN	PUNTAJE MAXIMO	PUNTAJE MINIMO	Kaspersky	with Secure	Crowdstrikes
1	Funcionalidad	Brindar un sistema de gestión centralizado de gestión Basado en nube e integrar al directorio activo para una gestión eficiente.	3	1	3	3	3
		Compatibilidad con sistemas operativos Windows, Linux, Mac, iOS.	3	1	3	3	3
		Debe incluir la integración de un sistema inventario de hardware y software con reconocimiento de vulnerabilidades a nivel parches.	3	1	3	3	3
		Debe incluir la gestión de parches de actualización multiplataforma.	3	1	3	3	3
		Debe incluir módulo de control de aplicaciones basado en listas blancas y listas negras.	3	1	3	3	3
		Debe incluir módulo de control de dispositivos con capacidad de configurar listas blancas basadas en ID del hardware.	3	1	3	3	3
		Deber incluir módulo de control de contenido web con capacidad de filtrar páginas web basadas en categorías.	3	1	3	3	3
		Debe incluir tecnología de detección basado en firmas, supervisión de conducta, inteligencia artificial y machine learning.	3	1	3	3	3
		Debe incluir funcionalidades que permitan explorar el performance de la red y tomar acciones preventivas ante comportamientos anómalos.	3	1	3	3	3

Oscar Berry

Edwin T.

SAT SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA	LEY 28612 LEY QUE NORMA EL USO, ADQUISICION Y ADECUACION DEL SOFTWARE EN LA ADMINISTRACION PUBLICA	Fecha: 07.03.2025
	INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE	Página 3 de 4

		Sistema de generación de informes y programación de envío de alertas.	3	1	3	3	3
2	Fiabilidad	Debe contar con soporte local 24x7 para asistencias presenciales y/o remotas por parte del postor o integrador.	6	0	6	6	5
		Debe contar con soporte local 24x7 para asistencias presenciales y/o remotas por parte del fabricante de forma local (2° Capa).	6	0	3	3	3
3	Usabilidad	Debe incluir un sistema de acceso a la consola de administración basado en perfiles.	4	0	4	4	4
		Consola de administración portable para acceso de técnicos en diferentes ubicaciones.	4	0	4	4	4
		Configuración especial para equipos de bajo performance.	4	0	3	3	3
		Posibilidad de solicitar permisos de acceso a web, aplicaciones y dispositivos desde el usuario	4	0	4	4	4
		Posibilidad de enviar mensajes de alertas en las pantallas de los usuarios	4	0	4	4	4
4	Adaptabilidad	Adaptabilidad a trabajos específicos sin necesidad de conocimientos previos avanzados de software	8	1	8	8	7
		Fácil recuperación y/o migración de infraestructura (Respaldo de base de datos).	8	1	8	8	8
5	Adecuación	Se adecua plenamente a las funciones requeridas.	8	1	8	8	8
			Puntaje Total		82	82	80

METRICAS: ATRIBUTOS DE USO							
Nº	ATRIBUTO	DESCRIPCIÓN	PUNTAJE MAXIMO	PUNTAJE MINIMO	Kaspersky	with Secure	Crowdstrikes
1	Capacitación	Se dispone con cursos estándares con evaluación y certificación técnica emitida por el fabricante o	4	0	4	4	4

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE

Página 4 de 4

		representante oficial único en el país.					
2	Seguridad	La solución no debe estar observada ni investigada en temas de posible filtración de información de cliente o incorporación de backdoors en sus sistemas.	5	0	5	5	5
3	Satisfacción	Se presenta una interfaz amigable a nivel de usuario la cual permite la participación del usuario en el proceso de remediación a una incidencia.	5	0	5	5	5
Puntaje Total						14	14

De los resultados de la evaluación, se puede observar que el producto With Secure y Kaspersky, son los más adecuados para la protección de los equipos de la institución.

8. Conclusiones

De acuerdo con la evaluación realizada, las mejores alternativas de software antivirus son los productos With Secure Elements Endpoint Protection y Kaspersky Endpoint Detection and Response Optimum. Por lo que se recomienda su adquisición debida que cumplen con lo mínimo requerido para la institución.

9. FIRMAS



Edwin Turín Avila
Especialista de Gestión de Operaciones de TI II
SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA



Cesar Edilberto Terry Ramos
Especialista de Gestión de Operaciones de TI III
SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LIMA