

	FORMATO	Código: GDIFO013
	INFORME PREVIO DE EVALUACION DE SOFTWARE	Revisión:00 Aprobado: JETIC Fecha: 2015.05.02 Página: 1 de 6

INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE

N° 001-2023-ETIC

SOFTWARE ANTIMALWARE

1. NOMBRE DEL AREA

Equipo Tecnologías de la Información y Comunicaciones

2. RESPONSABLE DE LA EVALUACION

Edwin Fidel Chuquillanqui Dominguez

3. CARGO

Especialista de Sistemas

4. FECHA

Lima, 04 de enero del año 2023.


5. JUSTIFICACION

En SEDAPAL, a través del Equipo de Tecnologías de la Información y Comunicaciones, tiene la necesidad de una solución antimalware, para evitar estar expuesto a riesgos de ciberataques con intentos maliciosos de accesos no autorizado a computadores, vulneración a los sistemas informáticos o penetración la red interna con la intención de causar daño o extraer información, destrucción o manipulación.

De experimentar SEDAPAL un ciberataque a sus sistemas informáticos se corre el riesgo de bloqueo en los sistemas, pérdida de datos, robo de la información lo que generaría la paralización de las operaciones parcial o totalmente, generando perdidas monetarias y de imagen institucional. Los atacantes con motivos delictivos buscan ganancias financieras a través del robo de datos o la interrupción del negocio.

En este contexto, SEDAPAL requiere con carácter de importancia alta potenciar la seguridad de su red y equipos de cómputo con nuevos componentes de seguridad que refuercen la seguridad y los protejan contra las nuevas amenazas de ciberataques. Para ello es necesario adquirir una solución de antimalware corporativo para proteger las estaciones de trabajo con tecnologías modernas de detección de amenazas, así como de herramientas de respuesta a detección de nuevas amenazas no conocidas para el ransomware y ataques del tipo día cero (no firmadas) que brinden una mejor protección ante estos ciberataques, así como herramientas de análisis contra el malware que protegen el correo electrónico corporativo y la navegación de Internet, recursos que hoy en día se han convertido en las principales herramientas de colaboración en las actividades laborales, y son los principales focos de los ciberdelincuentes para tratar de vulnerar la seguridad de las empresas.

Por lo expuesto y en el marco del cumplimiento a la Ley N° 28612 (Ley que norma el uso, adquisición y adecuación del software en la Administración Pública) y su reglamento, se ha

	FORMATO	Código: GDIFO013
	INFORME PREVIO DE EVALUACION DE SOFTWARE	Revisión:00 Aprobado: JETIC Fecha: 2015.05.02 Página: 2 de 6

elaborado el presente informe, para determinar el software que cumpla con las necesidades de la entidad, bajo los principios de neutralidad, vigencia tecnológica y libre competencia.

6. ALTERNATIVAS

Considerando los requerimientos de SEDAPAL, se ha buscado alternativas de software en el mercado que cumplan con los requerimientos mínimos. En ese sentido los productos de software a evaluar son los siguientes:

Producto	Fabricante	Licenciamiento
WithSecure Elements Endpoint Protection	WithSecure	Por usuario
Kaspersky Endpoint Detection and Response Optimum	Kaspersky	Por usuario
Symantec EndPoint Security	Brandon	Por usuario

7. ANÁLISIS COMPARATIVO TÉCNICO.

Basada en la Ley 28612 – Ley que norma el uso, adquisición y adecuación del software en la Administración Pública y su reglamento, el Decreto Supremo N° 024-2006-PCM; publicado el 24.05.2006.

- A. Propósito de la Evaluación.** - El propósito del presente análisis es realizar una evaluación del producto materia de la renovación.
- B. Identificador de Tipo de Producto.** - El producto materia de esta evaluación es el software que permita realizar lo especificado en el Ítem Justificación.
- C. Especificaciones de Modelo de Calidad.** - Se aplicará el Modelo de Calidad de Software descrito y aprobado por Resolución Ministerial N° 139-2004-PCM. En donde se determinaron las características y atributos mínimos que tendría el software, en base a la información técnica de los productos señalados en el **ítem 6. "Alternativas"**. En el **Cuadro 1** se detallan las características y atributos mínimos que se determinaron para el software a evaluar.
- D. Selección de Métricas.** - Las métricas fueron seleccionadas en base al análisis de información técnica solicitado por el Equipo Tecnologías de la Información y Comunicaciones.

7.1. MODELO DE CALIDAD:

A. Determinación de Atributos

Cuadro N° 01: Atributos a Evaluar

ITEM	ATRIBUTOS	DESCRIPCION	PUNTAJE
01	CALIDAD INTERNA Y EXTERNA		60
Funcionalidad			
1.1	Adecuación	Capacidad del software para adecuarse a la plataforma Windows en sus últimas versiones	3
	Exactitud	Protección proactiva Escaneado inteligente de equipos Eficacia en defender los sistemas contra virus, buffer overflows y ataques combinados. Capacidad para limitar el daño provocado por contagios. Bloqueo de amenazas que escriben en la memoria. Protección web.	3
	Interoperabilidad	Interacción con bases de datos Oracle, SQL, así como herramientas de Microsoft Office, navegadores de internet, Integración con el Directorio Activo.	3
	Funcionalidad mínima	La protección contra código espía y sus variantes debe ser en tiempo real minimizando todos los riesgos posibles de posible infección del punto final (estaciones de trabajo y servidores) no comprometiendo el rendimiento de éste. Administración centralizada. Control de aplicaciones (permitir o impedir la ejecución de aplicaciones de origen comercial o realizado por la entidad). Bloqueo de dispositivos en los puntos finales (estaciones de trabajo y servidores) para prevenir la fuga de datos.	5
	Seguridad	Capacidad para proteger información y datos. Proteger con contraseña la configuración del antimalware para que no sea alterada	3
Fiabilidad			
1.2	Madurez	Robustez para evitar fallas producto de errores en el software	4
	Tolerancia a errores	Capacidad para mantener un nivel específico, en caso de errores	3
Usabilidad			
1.3	Entendimiento	Facilidad, rapidez de comprensión a nivel usuario	4
	Idioma	Interfaz gráfica en idioma español	2
	Aprendizaje	Documentación pre y post instalación. Ayuda on-line	4
	Operabilidad	Acceso de fácil interpretación y/o visualización	4
Eficiencia			

1.4	Comportamiento de Tiempos	Alto rendimiento para análisis y procesos (velocidad de procesamiento)	3
	Utilización de Recursos	El software debe consumir recursos mínimos de la PC, sin afectar capacidad multitarea del procesador y memoria	3
Mantenimiento			
1.5	Actualización	Facilidad para migrar a versiones superiores. Actualización de firmas manuales y automáticas. Capacidad de uso de repositorios distribuidos.	3
	Soporte	Servicio técnico local garantizado	4
Portabilidad			
1.6	Adaptabilidad	Adaptable a diversos entornos	1
	Facilidad de Instalación	Contar con asistente de instalación	2
	Coexistencia	Convivencia con diferentes software sin causar conflictos	2
	Reemplazabilidad	Capacidad para ser utilizado en lugar de otro software estadístico, sin perder información, funcionalidades básicas y para los mismos propósitos	2
02	CALIDAD DE USO		10
2.1	Eficacia	Capacidad de alcanzar metas operativas/indicadores del usuario en contexto específico de uso	3
2.2	Seguridad	Capacidad de ser confiable y seguro para trabajo local o en red	3
2.3	Satisfacción	Capacidad para cubrir requerimientos con total conformidad del usuario	4
03	IMPLEMENTACION		10
3.1	Capacitación	Necesidad de capacitación para la administración del software. Existencia de centros de capacitación en el medio local	5
3.2	Impacto	Capacidad de reducir el impacto de la implementación de la solución	5

B. Análisis Técnico y Calificación

El análisis técnico y calificación de las métricas realizado a las alternativas de software se muestra en el siguiente cuadro:

Cuadro N° 02 Análisis Comparativo Técnico

ITEM	ATRIBUTOS		PUNTAJE	ALTERNATIVAS		
				WithSecure	Symantec	Kaspersky
01	ATRIBUTOS INTERNOS Y EXTERNOS		60			
1.1	Funcionalidad	Adecuación	3	3	3	3
		Exactitud	3	2	2	2
		Interoperabilidad	3	2	2	2

ITEM	ATRIBUTOS		PUNTAJE	ALTERNATIVAS		
				WithSecure	Symantec	Kaspersky
01	ATRIBUTOS INTERNOS Y EXTERNOS		60			
		Funcionalidad mínima	5	3	3	3
		Seguridad	3	2	3	3
1.2	Fiabilidad	Madurez	4	3	3	4
		Tolerancia a errores	3	2	3	3
1.3	Usabilidad	Entendimiento	4	4	4	4
		Idioma	2	2	2	2
		Aprendizaje	4	3	3	3
1.4	Eficiencia	Operabilidad	4	3	3	3
		Comportamientos de tiempos	3	2	2	3
1.5	Mantenimiento	Utilización de recursos	3	2	3	3
		Actualización	3	2	3	3
1.6	Portabilidad	Soporte	4	3	3	3
		Adaptabilidad	3	3	3	3
		Facilidad de instalación	2	2	2	2
		Coexistencia	2	2	1	1
		Reemplazabilidad	2	2	2	2
Sub-Total			60	47	50	52
02	ATRIBUTOS DE USO		10			
2.1	Eficacia		3	3	3	3
2.2	Seguridad		3	2	3	3
2.3	Satisfacción		4	1	2	2
Sub-Total			10	6	8	8
03	ATRIBUTOS DE IMPLEMENTACIÓN		10			
3.1	Capacitación		5	5	3	3
3.2	Impacto		5	5	5	5
Sub-Total			10	10	8	8
TOTAL			80	63	66	68

De esta manera se han evaluado las características técnicas de los productos mencionados y servicios adicionales, habiéndose verificado que cada uno de ellos cubre nuestras necesidades.

8. ANALISIS COSTO – BENEFICIO

Para la elaboración del análisis de costo beneficio se ha tomado en cuenta los criterios solicitados en el punto 8 del Reglamento de la Ley N° 28612.

Cuadro N° 03: Resumen de criterios de los productos

N°	Criterios a evaluar	WithSecure	Symantec	Kaspersky
1	Licenciamiento	Requerido	Requerido	Requerido
2	Costo Referencial x Licencia	S/ 245.00	S/ 149.00	S/ 138.00
3	Hardware necesario para su funcionamiento	SI	SI	SI
4	Soporte y mantenimiento externo	SI	SI	SI
5	Personal y mantenimiento interno	SI	SI	SI

A continuación, se presenta en el cuadro N° 4 el resultado global del análisis técnico y el análisis costo beneficio:

Cuadro N° 04 Resumen de Evaluación Global

ATRIBUTOS	WithSecure	Symantec	Kaspersky
Análisis Comparativo Técnico	63	66	68
Análisis Costo Beneficio	0.2571	0.4429	0.4564

9. CONCLUSIONES

- El Equipo de Tecnologías de la Información y Comunicaciones (ETIC) tiene la necesidad de contar con nuevas licencias de un software antimalware, dado que la solución actual asociada es una solución antivirus y adicionalmente esta por caducar en el corto plazo.
- Técnicamente las alternativas evaluadas cumplen con los requerimientos funcionales de la empresa.
- Algunos de los costos de las licencias de las marcas evaluadas han sido obtenidas utilizando internet, por lo que son referenciales y variables; resultando la solución de software antimalware Kaspersky la que presenta el menor costo unitario por licencia.
- En conclusión, por los motivos ya señalados, se recomienda adquirir el software antimalware Kaspersky Endpoint Detection and Response Optimum dado que cumple con el mayor número de características técnicas consideradas en la evaluación.

Atentamente,

Edwin Fidel Chuquillanqui Dominguez
Especialista de Sistemas

VB: Victor Guevara Chavez
Jefe Equipo Tecnología de la
Información y Comunicaciones (e)