INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE - SUSCRIPCIÓN DE LICENCIAS PARA UNA SOLUCIÓN DE PROTECCIÓN AVANZADA ANTIMALWARE PARA DISPOSITIVOS FINALES DEL OSITRAN

OSITRAN

Firmado por: GOMEZ BACILIO Everth Jesus FAU 20420248645 soft
Motivo: Firma Digital
Fecha: 29/09/2021 09:51:53 -0500

1. NOMBRE DEL AREA: Jefatura de Tecnologías de la Información.

2. NOMBRE Y CARGO DE LOS RESPONSABLES DE LA EVALUACIÓN:

- Everth Jesús Gómez Bacilio, Especialista en Redes y Telecomunicaciones II.
- Cesar Enrique Talledo, Jefe de Tecnologías de la Información.

3. FECHA: Lima,24 de setiembre de 2021

4. JUSTIFICACION:

Desde el año 2019, el OSITRAN utiliza para la protección de informática de los equipos y servidores la solución **CORTEX XDR Palo Alto** (452 licencias en ambas sedes), cuyo periodo de contratación para la actualización de parches, base de datos y firmas de virus caducará el 13 de noviembre de 2021, la cual viene trabajando de manera óptima en la protección de estaciones de trabajo, servidores y sistemas informáticos. Es necesario indicar que a la fecha la entidad continúa trabajando con el producto CORTEX XDR en todos los equipos.

Con el objetivo de garantizar la protección de los equipos y la información de la Institución, así como la continuidad de los servicios que permiten el cumplimiento de las labores de los usuarios, se requiere realizar la adquisición de licencias de una solución antimalware para los equipos informáticos de ambas sedes, que funcione con el mismo nivel de desempeño y características que la solución con la que cuenta actualmente el OSITRAN. En base a la información recabada y al crecimiento del parque informático se ha determinado que se requieren cuatrocientas (452) licencias. Las especificaciones técnicas requeridas son las siguientes:

5. ALTERNATIVAS:

Se han elegido las siguientes alternativas de software antimalware para su evaluación, en razón a las referencias sobre su desempeño y bajo impacto sobre el uso de recursos de procesamiento y memoria, así como la existencia de varios proveedores y de soporte en Perú a nivel nacional. No se han considerado alternativas de software libre, pues no cuenta con soporte técnico válido a nivel nacional.

- Trend Micro Office Scan for STD
- Cortex XDR Endpoint Protection and Response
- Kaspersky Endpoint Security for Business

6. ANÁLISIS COMPARATIVO TÉCNICO

6.1 Descripción de métricas

Nº	Atributo	Descripción	Puntaje Máximo	Criterio de Calificación	Puntaje
ATRIBUTOS INTERNOS					
1		Para estaciones de trabajo: Windows 7/8/10 y MacOS. Para Servidores:	6	Todos	6

	Sistemas operativos soportados	Windows Server 2008/2012/209, Linux (CentOS, Debian). Físicas y virtuales. Dispositivos Android.		Algunos	4
2	Seguridad y defensa contra malware	El software antimalware debe ser capaz de proteger contra virus, troyanos, gusanos, spyware, adware y otros tipos de malware.	6	Avanzado	6
				Intermedio	3
				Básico	1
3	Prevención	La solución debe detectar y prevenir virus, programas espías, rootkits, troyanos y programas publicitarios, así como aplicaciones no deseadas (PUA).	6	Avanzado	6
				Intermedio	3
				Básico	1
4	Recursos de sistema	CPU: < 1% CPU Memoria RAM: < 150MB Espacio HD: 250 MB	5	Avanzado	4
				Intermedio	3
				Básico	1
5	Consola de gestión de los agentes de protección	Consola alojada en nube. Enfoque de seguridad como servicio, optimiza recursos de infraestructura de los clientes y costos operativos en mantenimiento y administración de un servidor local, que incluso puede corromperse o fallar como todo hardware.	5	Si	5
				No	3
6	Consumo de ancho de banda	1000 agentes en promedio consumen 1.2 Mbps de forma concurrente. Es un valor directamente proporcional	5	Si	5
				No	3
		SUBTOTAL	33		
REQUERIMIENTOS MINIMOS					
7	Prevención de Exploits (Windows)	Enfocado en bloquear las técnicas de ataque en lugar de vulnerabilidades, es un enfoque más efectivo y óptimo que no vuelve lento al sistema.	4	Avanzado	4
				Intermedio	3
				Básico	1
8	Prevención de Exploits (MacOS y Linux)	Por lo menos 5 módulos de protección contra Exploits para MacOS y 3 para Linux. Es un enfoque diferente a Windows, ya que en Windows existen más variantes de explotación	4	Avanzado	4
				Intermedio	3
				Básico	1
9	0-day Exploits	Detección incorporada para todas las técnicas de explotación relevantes. No se requieren actualizaciones de las firmas	4	Avanzado	4
				Intermedio	3
				Básico	1
10	Prevención de malware conocido	Detección mediante comparación de Hash, comunicación instantánea con Nube, determinando con precisión la verdadera naturaleza del ejecutable. Debe ser una validación en línea y en tiempo real que no depende de la descarga de una base de datos de firmas de protección	4	Avanzado	4
				Intermedio	3
				Básico	1
11	Nube de Inteligencia de	Inteligencia de Amenazas y Sandbox Cloud. Base de datos que contiene miles de	4	Avanzado	4
				Intermedio	3

	Amenazas	millones de muestras y con promedio de muestras superior a 300 millones al mes.		Básico	1
12	Protección basada en comportamiento	Identifica o perfila el comportamiento habitual de un sistema, si un ejecutable intenta realizar un comportamiento anómalo, se bloqueará dicho proceso asociado al comportamiento malicioso	4	Avanzado	4
				Intermedio	3
				Básico	1
13	Restricción de procesos hijos maliciosos	Existen ataques basados en scripts ejecutados sobre programas legítimos (por ejemplo, Powershell) que intentan levantar procesos conocidos para eludir los mecanismos tradicionales de protección	4	Avanzado	4
				Intermedio	3
				Básico	1
14	Examinación de DDL's y PE (portables, ejecutables)	Analiza si un proceso malicioso está tratando de ejecutar DDL's corruptas durante la ejecución de una aplicación o software	4	Avanzado	4
				Intermedio	3
				Básico	1
15	Protección Offline	Algoritmo que usa Machine Learning que permite identificar malware conocido y desconocido. La herramienta debe contener este algoritmo localmente y se ejecuta sin necesidad de que el sistema tenga conexión a internet	5	Avanzado	5
				Intermedio	4
				Básico	1
16	Protección de malware desconocido	- Algoritmos basados en Machine Learning -Protección basada en comportamiento maliciosos - Sandboxing Cloud: el cual ejecuta el malware en un sistema operativo virtualizado y/o real (Bare Metal Analysis), ya que existe malware que se inhibe cuando detecta que lo intentan ejecutar en equipos virtuales. Sandboxing debe tener un tiempo de respuesta de 5 minutos para dar el veredicto de un archivo sospechoso.	5	Avanzado	5
				Intermedio	4
				Básico	1
17	Modulo Anti-ransomware	Capacidad de prevenir ante ataques de tipo ransomware que secuestren la información del usuario final.	5	Avanzado	5
				Intermedio	4
				Básico	1
		SUBTOTAL	47		
CARACTERISTICAS Y FUNCIONALIDADES ACCESORIAS					
18	Alertas y reportes	Informes personalizados disponible s para cada evento bloqueado, donde se puede ver procesos afectados, timeline de comportamiento malicioso, tipo de comportamiento en Windows, Linux, Mac, Android.	5	Total	5
				Parcial	3
19	Documentación	El software debe contener manuales de instalación y de configuración.	5	Total	5
				Parcial	3
20	Soporte técnico y capacitación	Se debe proporcionar soporte técnico en red y telefónico 24x7.	5	Si	5
				No	0
21	Usabilidad		5	Total	5

		El sistema de tener facilidad y rapidez de comprensión a nivel de usuario, con interfaz gráfica en español.		Parcial	3
		SUBTOTAL	20		

TOTAL	**100**
TOTAL MÍNIMO	**80**

6.2 Puntajes

Nº	Atributo	Puntaje Máximo	Criterio de Calificación	Puntaje	CORTEX XDR	TREND MICRO	KASPERSKY
ATRIBUTOS INTERNOS							
1	Sistemas operativos soportados	6	Todos	6	6	4	4
			Algunos	4			
2	Seguridad y defensa contra malware	6	Avanzado	6	6	6	6
			Intermedio	3			
			Básico	1			
3	Prevención	6	Avanzado	6	6	6	6
			Intermedio	3			
			Básico	1			
4	Recursos de sistema	5	Avanzado	5	5	3	3
			Intermedio	3			
			Básico	1			
5	Consola de gestión de los agentes de protección	5	Si	5	5	3	3
			No	3			
6	Consumo de ancho de banda	5	Si	5	5	3	3
			No	3			
	SUBTOTAL	33	SUBTOTAL		33	25	25
REQUERIMIENTOS MINIMOS							
7	Prevención de Exploits (Windows)	4	Avanzado	4	4	4	3
			Intermedio	3			
			Básico	1			
8	Prevención de Exploits (MacOS y Linux)	4	Avanzado	4	4	3	3
			Intermedio	3			
			Básico	1			
9	0-day Exploits	4	Avanzado	4	4	3	3
			Intermedio	3			
			Básico	1			
10	Prevención de malware conocido	4	Avanzado	4	4	4	4
			Intermedio	3			
			Básico	1			
11	Nube de Inteligencia de Amenazas	4	Avanzado	4	4	3	3
			Intermedio	3			
			Básico	1			
12	Protección basada en comportamiento	4	Avanzado	4	4	1	1
			Intermedio	3			
			Básico	1			
13	Restricción de	4	Avanzado	4	4	3	3
			Intermedio	3			

	procesos hijos maliciosos		Básico	1			
14	Examinación de DDL's y PE (portables, ejecutables)	4	Avanzado	4	4	3	3
			Intermedio	3			
			Básico	1			
15	Protección Offline	5	Avanzado	5	5	4	4
			Intermedio	4			
			Básico	1			
16	Protección de malware desconocido	5	Avanzado	5	5	4	4
			Intermedio	4			
			Básico	1			
17	Modulo Anti-ransomware	5	Avanzado	5	5	5	5
			Intermedio	4			
			Básico	1			
		47	SUBTOTAL		47	37	36
CARACTERISTICAS Y FUNCIONALIDADES ACCESORIAS							
18	Alertas y reportes	5	Total	5	5	3	5
			Parcial	3			
19	Documentación	5	Total	5	5	5	5
			Parcial	3			
20	Soporte técnico y capacitación	5	Si	5	5	5	5
			No	0			
21	Usabilidad	5	Total	5	5	5	5
			Parcial	3			
	SUBTOTAL	20	SUBTOTAL		20	20	20

TOTAL	**100**	**TOTAL**	**100**	**82**	**81**

7. COSTO TOTAL DE LICENCIAS:

CUADRO COMPARATIVO			
Adquisición de 400 licencias, actualización, mantenimiento y soporte por dos (02) años			
Producto	**CORTEX XDR Endpoint Advanced Protection**	**Trend Micro. Office Scan Standar**	**Kaspersky Endpoint Security for Business**
Hardware para consola de administración	No se requiere, consola en nube.	Servidor provisto por la institución	Servidor provisto por la institución
Soporte y mantenimiento externo	Incluido	Incluido	Incluido
Personal y mantenimiento interno	Personal de la institución	Personal de la institución	Personal de la institución
Capacitación	Incluido	Incluido	Incluido
Costo de licencias x Unidad	**S/. 220.00**	**S/. 195.00**	**S/. 209.00**
Costo de licencias TOTAL	**S/. 88,000.00**	**S/. 78,000.00**	**S/. 83,600.00**
Puntaje Ponderado por Costo	**88.63**	**100.00**	**93.30**

Nota: El Costo de las licencias es un precio referencial consultado en internet
http://computacion.mercadolibre.com.pe/antivirus
http://www.kernelsoftware.com/products/catalog/trend_micro.html

8. ANÁLISIS COMPARATIVO DE COSTO-BENEFICIO:

El presente análisis tiene por objetivo seleccionar la mejor alternativa. Para lo cual se ha optado por dar un peso a la evaluación técnica de **0.7** y a la evaluación económica de **0.3**, con el fin de garantizar que el software cumpla con las necesidades solicitadas.

Por tanto, el Puntaje Final (PF) sería el siguiente:

PF= ***0.7****(Puntaje Análisis Comparativo Técnico) + **0.3****(Ponderado Total Costo de Licencias)*

Aplicando dicha fórmula en las alternativas seleccionadas tenemos el siguiente puntaje final:

PF CORTEX XDR Endpoint Protection Advanced = *0.7*100 + 0.3*87.5 =* ***96.59***

PF Trend Micro OfficeScan *= 0.7*82 + 0.3*100 =* ***87.4***

PF Kaspersky Endpoint Security for Business *= 0.7*81 + 0.3*94.59 =* ***84.70***

9. CONCLUSIONES

Luego de la evaluación realizada se indica que los productos cumplen con las características mínimas solicitadas para el buen funcionamiento requerido en la Institución, siendo la solución de la marca **CORTEX XDR - Endpoint Protection**, que presenta mejor Costo/Beneficio a todo nivel.

10. FIRMAS

_____
Sr. Everth Gómez Bacilio
Especialista en Redes y Telecomunicaciones II

_____
Sr. Cesar Enrique Talledo León
Jefe de Tecnologías de la Información