LA CONTRALORÍA
GENERAL DE LA REPÚBLICA

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE N° 040-TI-2024-CGR

Firmado digitalmente por
INGA LOPEZ Wilder Alex FAU
20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 25-07-2024 18:16:21 -05:00

Firmado digitalmente por
BAZÁN FLORES Erik Ulises
FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 25-07-2024 19:12:00 -05:00

Firmado digitalmente por
ORTEGA CAMPANA Amparo FAU
20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 25-07-2024 19:34:42 -05:00

ÍNDICE

Firmado digitalmente por
INGA LOPEZ Wilder Alex FAU
20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 25-07-2024 18:16:21 -05:00

Firmado digitalmente por
BAZÁN FLORES Erik Ulises
FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 25-07-2024 19:12:00 -05:00

Firmado digitalmente por
ORTEGA CAMPANA Amparo FAU
20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 25-07-2024 19:34:42 -05:00

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE PARA LA ADQUISICIÓN DE SOLUCIÓN DE SOFTWARE DE SEGURIDAD INFORMÁTICA PARA LA PROTECCIÓN DE LOS DISPOSITIVOS DE LA CONTRALORÍA GENERAL DE LA REPÚBLICA DEL PERÚ

1. NOMBRE DEL ÁREA

Subgerencia de Sistemas de Información - Gerencia de Tecnologías de la Información.

2. NOMBRE Y CARGO DEL RESPONSABLE DE LA EVALUACIÓN

Erik Bazán Flores – Subgerente de Sistemas de Información

3. FECHA

24 de julio de 2024

4. JUSTIFICACIÓN

La Gerencia de Tecnologías de la Información (GTI), como encargada de dirigir y ejecutar las actividades relacionadas con las tecnologías de la información, la operatividad de los equipos de procesamiento de información, la seguridad informática y el correcto funcionamiento de la red de transmisión de comunicaciones que soporta los procesos de la CGR, ha contemplado la adquisición de una solución de seguridad con la finalidad de mejorar la seguridad informática de los datos e información generada, procesada y almacenada en servidores, estaciones de trabajo y dispositivos móviles que forman parte del parque informático de la institución a nivel nacional y de los diversos servicios de TI, así como para mejorar la “Gestión de la Seguridad de la Información”, “Gestión de Riesgos” y “Gestión de la Continuidad del Negocio” de la Institución.

Actualmente, la CGR cuenta con una solución de antivirus que brinda la protección de los datos e información generada, procesada y almacenada en las computadoras y servidores de la institución, lo que constituye un servicio de vital importancia para la gestión de la seguridad de la información y continuidad de operaciones de la Institución.

Cabe mencionar que muchas de las aplicaciones que se utilizan como parte del trabajo diario requieren acceso a Internet y además comparten información con otros equipos informáticos ubicados en otras sedes a nivel nacional. Estos mecanismos de trabajo generan riesgos para la institución que deben ser gestionados y mitigados adecuadamente, por lo que se requiere la adquisición de una solución de seguridad informática, a fin reducir dichos riesgos.

Por lo expuesto y el marco de Ley N° 28612 "Ley que norma el uso, adquisición y adecuación del software en la Administración Pública", se procede a evaluar software de seguridad informática para la protección de los dispositivos.

5. ALTERNATIVAS

Considerando la necesidad de la CGR se han buscado alternativas de software en el mercado, tomando en consideración la disponibilidad en el servicio de atención y de soporte local.

En ese sentido, la búsqueda ha dado como resultado los productos que se listan a continuación:

- Sophos (Intercept X Advanced)
- Kaspersky (Integrated Endpoint Security with EDR)
- Trendmicro (Apex One)

6. ANÁLISIS 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.

Propósito de evaluación

Firmado digitalmente por INGA LOPEZ Wilder Alex FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 25-07-2024 18:16:21 -05:00

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 25-07-2024 19:12:00 -05:00

Firmado digitalmente por ORTEGA CAMPANA Amparo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 25-07-2024 19:34:42 -05:00

Validar que las alternativas seleccionadas sean las más convenientes técnicamente para el uso de la CGR.

b. Identificar el tipo de producto
Software para la adquisición de solución de software de seguridad informática para la protección de los dispositivos

c. Identificación del modelo de calidad
Se aplicará el Modelo de Calidad de Software descrito en la parte I de la Guía de evaluación de software aprobado por Resolución Ministerial N° 139-2004-PCM.

d. **Selección de métricas.**
Las métricas fueron seleccionadas en base a las características técnicas descritas en el anexo N° 1 en ella se han evaluado atributos internos, externos y de uso.

Dada la criticidad en que los productos de software cumplan con los criterios técnicos requeridos, aquellos que, en la **evaluación técnica** no alcancen 80 puntos del puntaje total como mínimo, no serán considerados para el análisis posterior de costo beneficio.

7. 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 0.8 y a la evaluación económica de 0.2, con el fin de garantizar que el software a adquirir o suscribir cumpla con los requerimientos técnicos solicitados.

- Del Análisis Comparativo Técnico del anexo N° 1, los productos que han resultado con puntajes iguales o mayores a 80 puntos en la Evaluación Técnica, fueron considerados para el Análisis Comparativo de Costo – Beneficio, calificando los siguientes:

  - Sophos (Intercept X Advanced)
  - Trendmicro (Apex One)

- En el anexo N° 2, se muestran los resultados del Análisis Comparativo de Costo – Beneficio, así como el cuadro de valoración técnica – económica.

- La evaluación de estas alternativas incluye los costos de licencias, los cuales son referenciales y fueron obtenidos a través de cotizaciones, páginas web de los fabricantes u otras fuentes. Ver anexo N° 3.

Asimismo, en la presente evaluación se ha considerado lo siguiente:

- **Hardware necesario para su funcionamiento de las alternativas**
  La Gerencia de Tecnologías de la Información a través de su Subgerencia de Operaciones y Plataforma Tecnológica ha determinado que no es necesaria la adquisición del hardware para el funcionamiento de los productos en mención.

- **Soporte y mantenimiento externo**
  Con la adquisición o suscripción de las licencias de los productos evaluados, se tienen derechos de soporte, actualizaciones de los parches y actualizaciones a versiones últimas liberadas por el fabricante durante el periodo de la garantía de los productos en mención.

- **Personal y mantenimiento interno**
  La CGR cuenta con soporte de Mesa de Ayuda a cargo de la Gerencia de Tecnologías de la Información, para realizar la instalación y configuración del software en los usuarios finales, así como para atender incidentes que pueda ocasionar el producto durante su funcionamiento.

- **Capacitación**
  El personal de las unidades orgánicas de la CGR, quienes utilizarán los productos evaluados, requerirá capacitación en función de sus necesidades.

CONTRALORÍA V°B°
Firmado digitalmente por INGA LOPEZ Wilder Alex FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 25-07-2024 18:16:21 -05:00

CONTRALORÍA V°B°
Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 25-07-2024 19:12:00 -05:00

CONTRALORÍA V°B°
Firmado digitalmente por ORTEGA CAMPANA Amparo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 25-07-2024 19:34:42 -05:00

8. CONCLUSIÓN

De los resultados del análisis realizado, se puede observar que los siguientes productos de software:

- Sophos (Intercept X Advanced)
- Trendmicro (Apex One)

Obtienen una valoración Costo/Beneficio que les permite cumplir con los requisitos mínimos solicitados y por ende con las necesidades de la institución.

9. FIRMAS

CONTRALORÍA
GENERAL DE LA REPÚBLICA DEL PERÚ

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Soy el autor del documento
Fecha: 25-07-2024 19:11:28 -05:00

Erik Bazán Flores
Subgerente de Sistemas de Información

V°B°

Firmado digitalmente por INGA LOPEZ Wilder Alex FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 25-07-2024 18:16:21 -05:00

V°B°

Firmado digitalmente por ORTEGA CAMPANA Amparo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 25-07-2024 19:34:42 -05:00

ANEXO N° 1

METRICAS (ATRIBUTOS) INTERNAS Y EXTERNAS								
N°	Atributos	Descripción	Puntaje Máximo	Criterio de Evaluación	Puntaje	Sophos	Kaspersky	Trendmicro
1	Funcionabilidad	Compatible con Windows 7 y posteriores, MacOS, Windows Server, Red Hat Enterprise, Ubuntu, CentOS, Android, IOS, Vmware, vSphere, Lotus Domino	3	Total	3	3	1	3
				Parcialmente	1			
		Proteger servidores, estaciones de trabajo y dispositivos móviles en tiempo real, bajo demanda o programado para detectar, bloquear y limpiar todos los virus, troyanos, gusanos, adware, spyware y malware en general, incluidos ransomware y malware de día cero. En Windows, el agente también debe detectar aplicaciones potencialmente indeseables (PUA), adware y comportamiento sospechoso.	3	Total	3	3	3	3
				Parcialmente	1			
		Permite exclusiones de escaneo para un determinado sitio web, archivo o carpeta, aplicación o proceso. Tanto a nivel global, como específico en cada política.	3	Total	3	3	1	3
				Parcialmente	1			
		Permite la sincronización con directorio activo (DA) para la gestión de usuarios y grupos integrados en las políticas de protección	3	Total	3	3	1	3
				Parcialmente	1			
		El agente proporciona control de amenazas, control de dispositivos, control de aplicaciones y control web.	3	Total	3	3	3	3
				Parcialmente	1			
		Detecta el malware en pre-ejecución y comprobar el comportamiento malicioso para detectar malware desconocido.	3	Total	3	3	3	3
				Parcialmente	1			
		Realiza la verificación de todos los archivos accedidos en tiempo real, incluso durante el proceso de arranque.	3	Total	3	3	1	3
				Parcialmente	1			
		Realiza la limpieza del sistema automáticamente, eliminando o poniendo en cuarentena elementos maliciosos detectados y PUA.	3	Total	3	3	3	3
				Parcialmente	1			
		Protege las funciones críticas en los navegadores de internet, incluida protección contra sitios web que realizan ataques de phishing.	3	Total	3	3	1	3
				Parcialmente	1			
		Posee un mecanismo de protección contra la desinstalación de la solución por el usuario.	3	Total	3	3	1	3
				Parcialmente	1			
		Utiliza una contraseña de protección para posibilitar la reconfiguración local en el cliente, deshabilitación temporal o desinstalación de los componentes de protección.	3	Total	3	3	1	3
				Parcialmente	1			
		Detecta el comportamiento sospechoso de las aplicaciones, tales como desbordamiento de búfer.	3	Total	3	3	1	3
				Parcialmente	1			
		Previene el ataque de vulnerabilidades de navegador a través de web exploits, o vulnerabilidades conocidas o de día cero.	3	Total	3	3	3	3
				Parcialmente	1			
		Administra como mínimo los siguientes dispositivos: discos duros externos, USB, CD, DVD, Blu-ray, interfaces de red inalámbrica, módems, bluetooth, infrarrojo, MTP (Media Transfer Protocol) y PTP (Picture Transfer Protocol) como cámaras digitales.	3	Total	3	3	3	3
				Parcialmente	1			
		Controla las aplicaciones para monitorear e impedir que los usuarios ejecuten o instalen aplicaciones que puedan afectar la productividad o el rendimiento de la red.	3	Total	3	3	3	3
				Parcialmente	1			
		El instalador debe permitir la instalación del cliente a través del directorio activo (DA) para múltiples equipos.	3	Total	3	3	1	3
				Parcialmente	1			
		El control web controla el acceso a sitios inapropiados, con categorías de sitios inadecuados. También debe permitir la creación de listas blancas y listas negras.	3	Total	3	3	3	3
				Parcialmente	1			
		Controla los siguientes archivos: Adjuntos en el cliente de correo , Adjuntos en el navegador (al menos IE, Firefox y Chrome), Adjuntos en el cliente de mensajería instantánea, dispositivos de almacenamiento (al menos USB, CD / DVD).	3	Total	3	3	1	3
				Parcialmente	1			
		Tiene capacidad de detección y bloqueo proactivo de keyloggers y otros malwares no conocidos (ataques de día cero) a través del análisis de comportamiento de procesos en memoria.	3	Total	3	3	3	3
				Parcialmente	1			
		Tiene capacidad de detección y bloqueo de troyanos, worms, entre otros malwares, por comportamiento de los procesos en memoria y genera excepciones ante falsos positivos.	3	Total	3	3	1	3
				Parcialmente	1			
		Mitiga la inyección de códigos en procesos, bloques de código malicioso, intentos de instrusión, ofrece protección contra robo de credenciales y contra malware en aplicaciones legítimas.	3	Total	3	3	3	3
				Parcialmente	1			
		Impide la migración de procesos maliciosos, evitando que un proceso malicioso migre a otro y evitando obtener escalamiento de privilegios, así como la modificación de las claves de registro para la ejecución de código arbitrario.	3	Total	3	3	1	3
				Parcialmente	1			
		Capacidad de protección contra ransomware incluido el sector de booteo, no basada exclusivamente en la detección por firmas, remediando la acción de encriptación maliciosa de los ransomware.	3	Total	3	3	1	3
				Parcialmente	1			
		Restaura automáticamente los archivos cifrados por un proceso malicioso de ransomware o debe evitar el cifrado de archivos por procesos maliciosos, informando a la consola todo el detalle del incidente para analizar la causa raíz de manera efectiva.	3	Total	3	3	1	3
				Parcialmente	1			
		Al menos en sistemas operativos Windows, el agente deberá contar con la funcionalidad de detección y respuesta del endpoint (EDR), opcionalmente esta funcionalidad estará disponible en Linux.	3	Total	3	3	3	3
				Parcialmente	1			
		Realiza la detección de "Root", de "Jailbreak" y protege contra Malware y PUA.	3	Total	3	3	1	3
				Parcialmente	1			
2	Fiabilidad	Soporte local, telefónico, correo, entre otros	3	Si	3	3	3	3
				No	0			
3	Usabilidad	Cuenta con herramientas de autoayuda o autoaprendizaje	3	Total	3	3	3	3
				Limitado	1			
4	Capacidad de mantenimiento	Se adapta a los cambios o mejoras de nuevas versiones	3	Total	3	3	3	3
				Parcialmente	1			
		Sub Total	87			87	57	87
METRICAS (ATRIBUTOS) DE USO								
5	Eficacia	Monitorea y controla dispositivos extraíbles en los equipos de los usuarios, como dispositivos USB, periféricos de la propia estación de trabajo y redes inalámbricas, aplicando estas políticas tanto por usuarios como por equipo.	3	Total	3	3	3	3
				Parcialmente	1			
6	Productividad	El agente no debe perder la comunicación con la consola de administración, a pesar que, el equipo donde se encuentre instalado el agente cambie de dirección IP o no se encuentren conectados a la red de la CGR	3	Total	3	3	3	3
				Parcialmente	1			
7	Accesibilidad	Realiza análisis forense de lo sucedido, para detectar la causa raíz del problema con el detalle de los procesos y sub-procesos ejecutados, la lectura y escritura de archivos y de las claves de registro. Debe incluir un registro de distintos equipos que hayan sido infectados por la misma amenaza.	3	Total	3	3	1	3
				Parcialmente	1			
8	Satisfacción	Conocimiento y confianza del usuario al Software	4	Totalmente	4	2	2	2
				Aceptable	2			
		Sub Total	13			11		11
		Total	100			98		98

CONTRALORÍA V°B°

Firmado digitalmente por INGA LOPEZ Wilder Alex FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 25-07-2024 18:16:21 -05:00

CONTRALORÍA V°B°

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 25-07-2024 19:12:00 -05:00

CONTRALORÍA V°B°

Firmado digitalmente por ORTEGA CAMPANA Amparo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 25-07-2024 19:34:42 -05:00

ANEXO N° 2
ANÁLISIS COMPARATIVO COSTO BENEFICIO

Información de costo anual obtenidos del mercado considerando mil dispositivos

Descripción	Costo total de la solución (S/.)
Sophos (Intercept X Advanced)	105,714.00
Trendmicro (Apex One)	79,285.50

Equivalencia del costo

Costo Total (S/)	Puntaje Equivalente
[0 -125,000>	100
[125,000 - 250,000>	85
+ de 250,000	50

Evaluación económica

Software	Costo Total 1 año (S/.)	Evaluación Económica
Sophos (Intercept X Advanced)	105,714.00	100
Trendmicro (Apex One)	79,285.50	100

Análisis costo beneficio

Software	Evaluación Técnica	Evaluación Técnica al 80% (A)	Evaluación Económica	Evaluación Económica al 20% (B)	Costo / Beneficio (A+B)
Sophos (Intercept X Advanced)	98	78.4	100	20	98.4
Trendmicro (Apex One)	98	78.4	100	20	98.4

Firmado digitalmente por INGA LOPEZ Wilder Alex FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 25-07-2024 18:16:21 -05:00

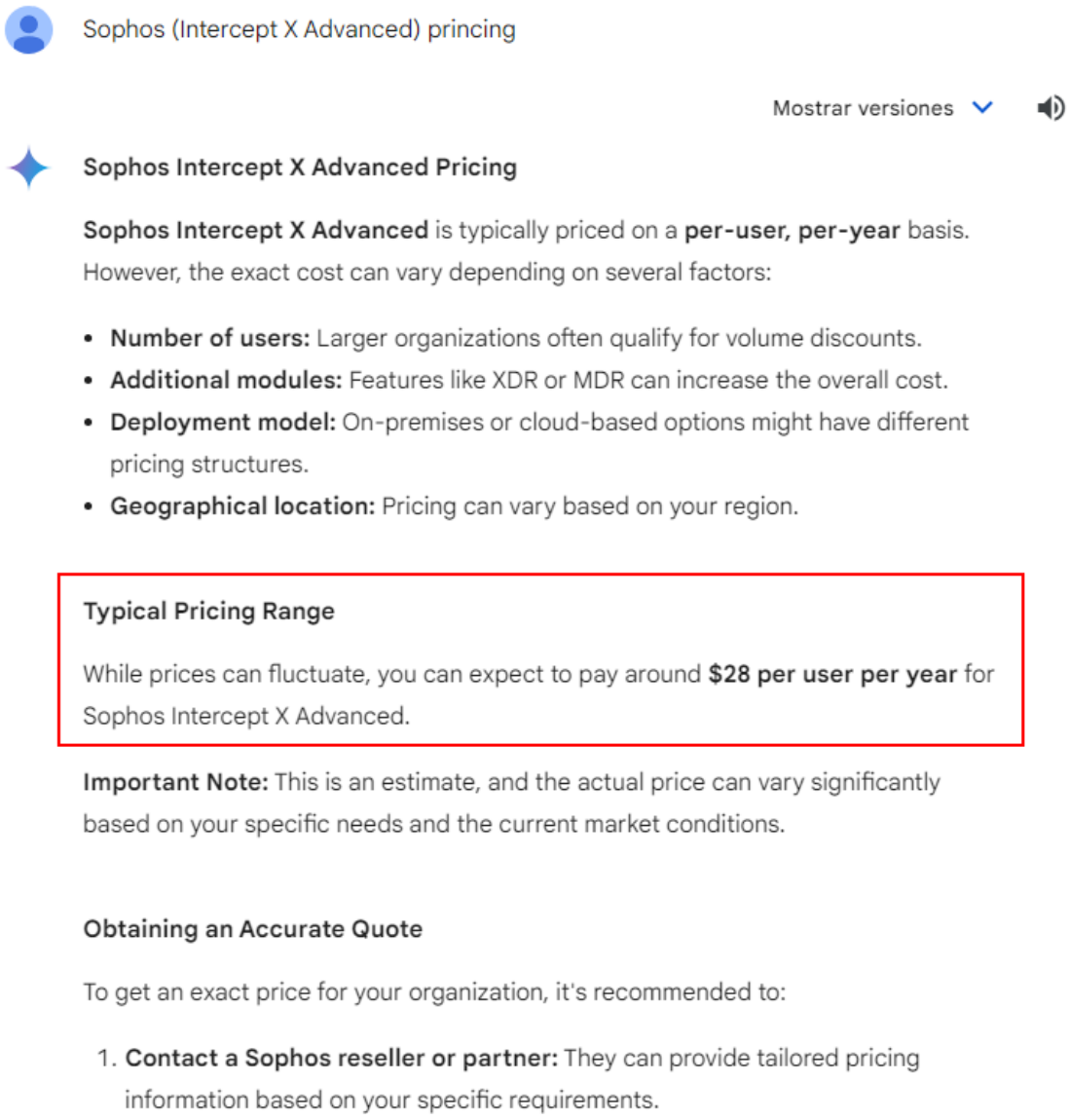
Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 25-07-2024 19:12:00 -05:00

Firmado digitalmente por ORTEGA CAMPANA Amparo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 25-07-2024 19:34:42 -05:00

ANEXO N° 3
COSTOS REFERENCIALES DE LICENCIAS DE SOFTWARE

a) Software Sophos (Intercept X Advanced)

Costo Total: S/. 105,714.00



Sophos (Intercept X Advanced) princing

Mostrar versiones

Sophos Intercept X Advanced Pricing

Sophos Intercept X Advanced is typically priced on a **per-user, per-year** basis. However, the exact cost can vary depending on several factors:

- **Number of users:** Larger organizations often qualify for volume discounts.
- **Additional modules:** Features like XDR or MDR can increase the overall cost.
- **Deployment model:** On-premises or cloud-based options might have different pricing structures.
- **Geographical location:** Pricing can vary based on your region.

Typical Pricing Range

While prices can fluctuate, you can expect to pay around **$28 per user per year** for Sophos Intercept X Advanced.

Important Note: This is an estimate, and the actual price can vary significantly based on your specific needs and the current market conditions.

Obtaining an Accurate Quote

To get an exact price for your organization, it's recommended to:

1. **Contact a Sophos reseller or partner:** They can provide tailored pricing information based on your specific requirements.

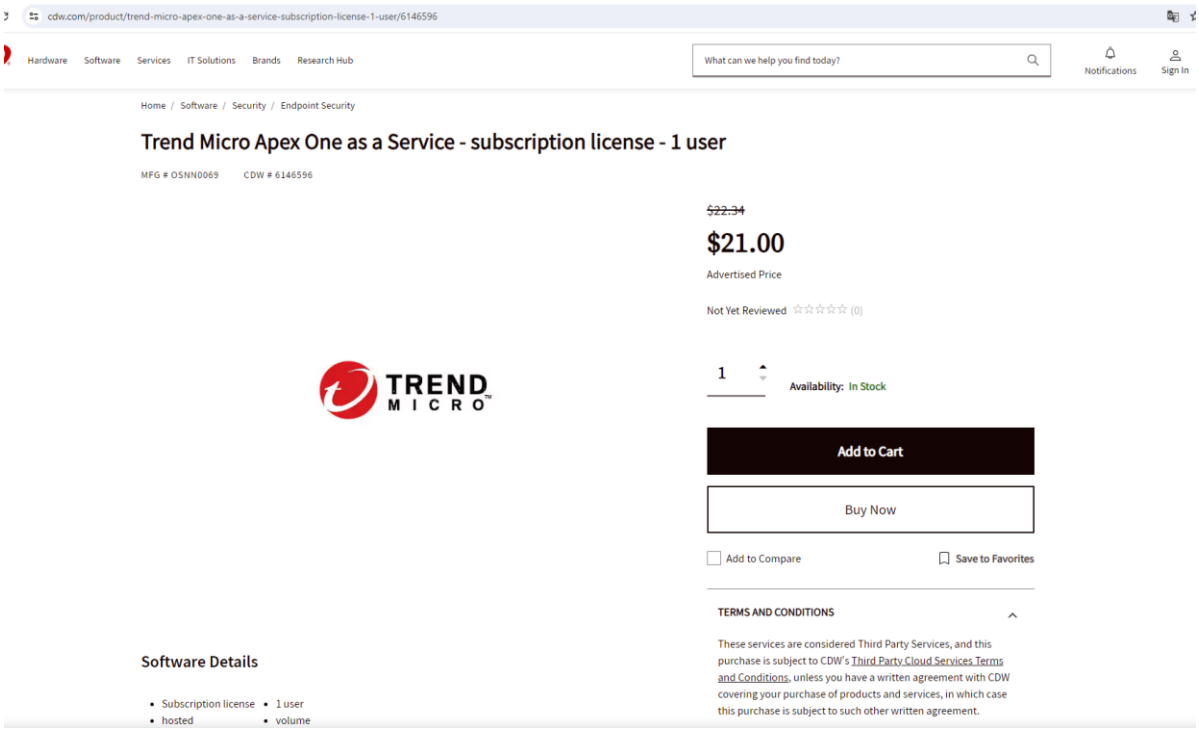
Fuente: https://gemini.google.com/app/03497c0dd5a01381 (acceso 25JUL2024 11:24)
(*) Tipo de cambio SBS al 24/07/2024: 3.7755

Firmado digitalmente por INGA LOPEZ Wilder Alex FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 25-07-2024 18:16:21 -05:00

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 25-07-2024 19:12:00 -05:00

Firmado digitalmente por ORTEGA CAMPANA Amparo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 25-07-2024 19:34:42 -05:00

b) Trendmicro (Apex One)
Costo Total: S/. 79,285.5



Fuente: https://www.cdw.com/product/trend-micro-apex-one-as-a-service-subscription-license-1-user/6146596 (Acceso 25JUL2024 15:23)
(*) Tipo de cambio SBS al 24/07/2024: 3.7755

Firmado digitalmente por INGA LOPEZ Wilder Alex FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 25-07-2024 18:16:21 -05:00

Firmado digitalmente por BAZÁN FLORES Erik Ulises FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 25-07-2024 19:12:00 -05:00

Firmado digitalmente por ORTEGA CAMPANA Amparo FAU 20131378972 soft
Motivo: Doy Visto Bueno
Fecha: 25-07-2024 19:34:42 -05:00