BANCO CENTRAL DE RESERVA DEL PERÚ

INFORME Nº 0111-2023-GTI230-N

Informe técnico previo de evaluación de software - Suscripciones de software de protección antimalware

1. NOMBRE DEL ÁREA:

Dpto. de Ciberseguridad y Redes

2. RESPONSABLE DE LA EVALUACIÓN:

Josue Asurza Caceres

3. CARGO:

Especialista en Ciberseguridad

4. JUSTIFICACIÓN:

Debido a la constante evolución de malware, gusanos, troyanos, ransomware y otros programas maliciosos, que se han vuelto más sofisticados y destructivos, las soluciones antivirus convencionales no ofrecen una protección suficiente para el entorno de seguridad informática que se mantiene cambiante y con nuevas necesidades cada año.

Los productos de protección antimalware para ataques informáticos han evolucionado y se han agregado componentes para garantizar la seguridad de las empresas. Estos incluyen, por citar algunos componentes, firewall endpoint, sistemas de prevención de intrusiones en el host (HIPS), control de dispositivos removibles, control de uso de aplicaciones y navegación web, detección automática de phishing, módulos de consultas de reputación en tiempo real, módulos de detección por comportamiento, cifrado de archivos o unidades de disco críticas y capacidad de integración a plataformas virtuales con el hipervisor designado.

La gestión y administración de las soluciones mencionadas se lleva a cabo desde una consola centralizada, que permite la aplicación de políticas, programación de tareas, la generación de informes de estado y la notificación de eventos en tiempo real.

En la actualidad el Banco administra tecnologías de seguridad con las características antes descritas a través de una solución antimalware de la marca Kaspersky.

5. ALTERNATIVAS:

Consideramos las siguientes marcas, que brindan soluciones de protección antimalware:

- ✓ Kaspersky
- ✓ Trellix
- ✓ ESET

6. ANÁLISIS COMPARATIVO TÉCNICO:

El análisis técnico ha sido realizado de conformidad con la metodología establecida en el documento "Guía Técnica sobre evaluación de software en la administración pública" (Resolución Ministerial N° 139-2004-PCM), tal como se exige en el reglamento de la Ley N° 28612.

a. Propósito de evaluación
Comparar alternativas de productos existentes en el mercado.

b. Identificar el tipo de producto
Solución de control de acceso a red.

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 RM N° 139-2004-PCM.

d. Selección de métricas.
Las métricas fueron seleccionadas en base a las características técnicas descritas en el Anexo N° 1.

Según el análisis realizado, la única marca que cumple lo requerido es Kaspersky.

7. ANÁLISIS COMPARATIVO DE COSTO – BENEFICIO:

Beneficios:

- Protección antimalware a base de firmas para la identificación en tiempo real de amenazas conocidas.
- Protección antimalware avanzada basada en comportamiento para la identificación en tiempo real de nuevas amenazas en red.
- Protección antimalware avanzada basada en reputación vía análisis de nube para la identificación en tiempo real de nuevas amenazas externas a la red.
- Consola de Web y MMC para gestión de la solución con capacidad de generación de reportes estadísticos.
- Asegura la compatibilidad con el componente Kaspersky Endpoint Agent (KEA), versión 3.13, del servicio de detección y respuesta ante amenazas.

Costos:

Las prestaciones requeridas corresponden al periodo de siete (07) meses de servicio:

- Prestación principal: Suscripción a los servicios del fabricante
  Suscripciones de software de protección antimalware Kaspersky.

- Prestación accesoria: Servicios del partner (proveedor local)
  Mesa de ayuda y soporte presencial, en el esquema 24x7 y mantenimiento técnico preventivo.

En base a las cotizaciones referenciales obtenidas se estima que el costo del servicio se encuentra dentro del margen presupuestado en PAC 2023.

8. CONCLUSIONES:

Por lo expuesto anteriormente, se considera conveniente la contratación de suscripciones de software de protección antimalware, por el periodo de siete (07) meses.

BANCO CENTRAL DE RESERVA DEL PERÚ

ANEXO N° 1

ATRIBUTOS Y MÉTRICAS

N°	Atributos	Puntaje máximo	Kaspersky	Trellix	ESET
1	Protección Antimalware	10	9	8	8
2	Protección contra ransomware	10	9	8	9
3	Detección por comportamiento	10	9	9	8
4	Protección de amenazas de red	10	9	8	9
5	Control de dispositivos removibles	10	9	0	8
6	Protección para estaciones Windows	10	9	8	8
7	Protección para servidores Windows y Linux	10	8	9	8
8	Protección para entornos virtuales VMware	10	7	8	8
9	Consola de gestión centralizada	10	10	10	10
10	Compatibilidad garantizada por el fabricante Kaspersky con Kaspersky Endpoint Agent (KEA) versión 3.13	10	10	0	0
Puntaje Total		100	89	68	76

*Indispensable para garantizar la operatividad de dicho módulo, el mismo que forma parte de otro servicio con contrato vigente (Servicio de detección y respuesta ante amenazas)

Lima, 21 de junio de 2023

cc.

BANCO CENTRAL DE RESERVA DEL PERÚ

FIRMADO POR:

Josue David ASURZA CACERES
Especialista en Ciberseguridad
Departamento de Ciberseguridad y Redes

Alexander John Anthony GAMBOA INGA
Jefe de Departamento de Ciberseguridad y Redes Interino
Departamento de Ciberseguridad y Redes
Firma como encargado.

VISADO POR:

Miguel Angel TEJADA MALASPINA
Subgerente de Servicios de Tecnologías de Información
Subgerencia de Servicios de Tecnologías de Información

Marco Antonio GRANADINO CACERES
Subgerente de Riesgos de Tecnologías de Información
Subgerencia de Riesgos de Tecnologías de Información

Miguel Angel TEJADA MALASPINA
Gerente de Tecnologías de Información Interino
Gerencia de Tecnologías de Información
Firma como encargado.

Javier Ernesto OLIVERA VEGA
Gerente Central de Administración
Gerencia Central de Administración