

BANCO CENTRAL DE RESERVA DEL PERÚ

INFORME N° 0002-2024-GTI420-N

Informe Técnico Previo de Evaluación de Software - Suscripciones de Protección de Nueva Generación para Endpoints (Next Generation Antimalware)

1. NOMBRE DEL ÁREA:

Departamento de Seguridad Informática

2. RESPONSABLE DE LA EVALUACIÓN:

Christian Manuel García Cerna
Alexander John Anthony Gamboa Inga
Marco Antonio Granadino Caceres

3. CARGOS:

Especialista en Seguridad Informática
Jefe de Departamento de Seguridad Informática (i)
Subgerente de 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 Instituciones. Estos incluyen, por citar algunos componentes módulos de detección por comportamiento e inteligencia artificial, correlación de alertas de forma automática, módulo de detección de analítica en base al framework MITRE, capacidades de threat hunting, capacidades de respuesta ante amenazas y capacidad para recolectar fuentes de terceros tales como firewalls perimetrales y controlador de dominio.

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

5. ALTERNATIVAS:

En esta evaluación hemos considerado las siguientes marcas, que brindan soluciones de protección de nueva generación para endpoints:

- ✓ Palo Alto Networks.
- ✓ CrowdStrike.

BANCO CENTRAL DE RESERVA DEL PERÚ

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.

7. ANÁLISIS COMPARATIVO DE COSTO – BENEFICIO:

Beneficios:

- Protección antimalware avanzada basada en comportamiento e inteligencia artificial 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.
- Bloqueos contra intentos de explotación de vulnerabilidades a sistemas no parchados e intentos de exploits 0-day.
- Consola de administración en la nube con capacidad de generación de reportes estadísticos.
- Consola de administración en la nube con capacidad para realizar threat hunting y respuesta ante amenazas.
- Capacidad para coleccionar fuentes de terceros y correlacionarlos.

Costos:

Las prestaciones requeridas corresponden al periodo de dos (02) años de servicio:

- Prestación principal: Suscripción a los servicios del fabricante
Suscripciones de Protección de Nueva Generación para Endpoints (Next Generation Antimalware).
- Prestación accesorio: Servicios del partner (proveedor local)
Mesa de ayuda y soporte presencial, en el esquema 24x7 y mantenimiento técnico preventivo.

BANCO CENTRAL DE RESERVA DEL PERÚ

En base a las cotizaciones referenciales obtenidas se estima que el costo del servicio se encuentra dentro del margen presupuestado en PAC 2024.

8. CONCLUSIONES:

Por lo expuesto anteriormente, se recomienda la contratación de suscripciones de Protección de Nueva Generación para Endpoints (Next Generation Antimalware), por el periodo de dos (02) años.

BANCO CENTRAL DE RESERVA DEL PERÚ

ANEXO N° 1

ATRIBUTOS Y MÉTRICAS

N°	Atributos	Puntaje máximo	Palo Alto Networks	CrowdStrike
1	Protección Antimalware	10	10	10
2	Protección contra ransomware	10	10	10
3	Detección por comportamiento	10	10	10
4	Control de dispositivos removibles	10	10	10
5	Protección para estaciones Windows	10	10	10
6	Protección para servidores Windows y Linux	10	10	10
7	Capacidad de Threat Hunting	10	10	09
8	Capacidad de respuesta ante incidentes	10	10	09
9	Capacidad de correlación de alertas	10	10	10
10	Capacidad de recolectar fuentes de terceros.	10	10	10
11	Efectividad de al menos 95% en detección de técnicas de ataque según el reporte de MITRE ATT&CK Evaluations en el 2023	10	10	10
12	Consola de gestión centralizada	10	10	10
Puntaje Total		120	120	118

Lima, 4 de abril de 2024

cc.

BANCO CENTRAL DE RESERVA DEL PERÚ

FIRMADO POR:

VISADO POR: