BANCO CENTRAL DE RESERVA DEL PERÚ

INFORME Nº 0048-2019-GTI230-N

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

---

1. NOMBRE DEL ÁREA:

Dpto. de Redes, Telecomunicaciones y Bases de Datos

2. RESPONSABLE DE LA EVALUACIÓN:

Alexander Gamboa Inga

3. CARGO:

Especialista en Redes, Telecomunicaciones y Bases de datos

4. JUSTIFICACIÓN:

Ante la constante evolución de virus, worms, trojan horses y otros programas maliciosos que se han vuelto cada vez más complejos y destructivos, las herramientas antivirus convencionales no son suficientemente capaces de proporcionar una protección adecuada.

Por tanto la tecnología de protección también ha evolucionado y nuevos componentes han sido adicionados, además del módulo de protección antimalware, incluyéndose otros módulos como firewall personal, HIPS (Host Intrusion Prevention System), protección para el acceso web, protección para el cliente de correo electrónico, control de dispositivos removibles, control de uso de aplicaciones e incluso DLP (Data Loss Prevention).

Debido al uso extendido de las plataformas de virtualización, por las ventajas que presentan en cuanto al uso más eficiente de los recursos hardware y facilidades de administración, los mecanismos de protección han debido de adecuarse a dichos entornos, lo que ha llevado a la aparición de una nueva generación de productos con integración a nivel del hipervisor.

En lo que respecta al correo electrónico, existen módulos de protección especializados para dicho servicio, a nivel del servidor y no sólo a nivel del cliente de correo.

La gestión de estas soluciones se realiza desde una consola centralizada, que permite la aplicación de políticas, generación de reportes de estado y notificación de eventos.

El uso de estas herramientas de protección debe complementarse con una adecuada política de seguridad que incluya la permanente educación de los usuarios respecto a las amenazas a que se exponen los recursos informáticos, tal como se recomienda en la Norma Técnica Peruana NTP-ISO/IEC 17799 2007, numeral 10.4.1 (Medidas y controles contra software malicioso), que establece: "*Se*

deberían implantar controles para detectar el software malicioso y prevenirse contra él, junto a procedimientos adecuados para concientizar a los usuarios."

5. ALTERNATIVAS:

En el mercado local se han encontrado productos de diversos fabricantes que cuentan con suites de productos que proporcionan las siguientes funcionalidades:

- ✓ Protección para equipos físicos (desktops y laptops).
- ✓ Protección especializada para la infraestructura virtual.
- ✓ Protección especializada para Microsoft Exchange.
- ✓ Consola de administración integrada.

Dentro de las alternativas existentes en el mercado que satisfacen los requerimientos hemos evaluado soluciones de los siguientes fabricantes:

(1) Kaspersky

(2) TrendMicro

(3) Symantec

6. ANÁLISIS COMPARATIVO TÉCNICO:

A continuación se presenta un cuadro referencial de cumplimiento de requerimientos generales.

	Especificaciones técnicas	(1)	(2)	(3)
Estaciones físicas (desktops y laptops)	Versiones para Windows y Mac OSX	SI	SI	SI
	Antimalware en tiempo real	SI	SI	SI
	Firewall personal	SI	SI	SI
	HIPS	SI	SI	SI
	Protección para el acceso web	SI	SI	SI
	Control de dispositivos removibles	SI	SI	SI
Entornos virtuales (servers y desktops)	Certificado para VMware NSX	SI	SI	SI
	Compatible con Citrix XenDesktop ejecutado en VMware vSphere	SI	SI	SI
	Protección antimalware	SI	SI	SI
Servidores de correo electrónico	Soporte de Microsoft Exchange 2013	SI	SI	SI
	Protección antispam	SI	SI	SI
	Protección antimalware	SI	SI	SI
Gestión	Gestión de políticas	SI	SI	SI
	Instalación remota de agentes	SI	SI	SI
	Reportes sobre el estado de la protección antimalware	SI	SI	SI

7. ANÁLISIS COMPARATIVO DE COSTO – BENEFICIO:

Beneficios:

- ➢ Protección para las estaciones físicas, entornos virtuales y para el servicio de correo electrónico.

- Consola centralizada para la gestión de la solución y generación de reportes.

Costos:

- Suscripción a los servicios del fabricante
  Actualizaciones de software (incluyendo el suministro de nuevas versiones y patches) y soporte técnico del fabricante (escalamiento), por el periodo de tres (03) años.

- Servicios del partner (proveedor local)
  Mesa de ayuda y soporte presencial, en el esquema 24x7x2, capacitación y mantenimientos técnicos preventivos.

- Hardware necesario para su funcionamiento
  El software antimalware solicitado se integrará a la plataforma informática con la que cuenta el BCRP.

En lo que respecta a los costos asociados, se consiguieron cotizaciones referenciales por S/ 335 876,65, S/ 590 310,58 y S/ 619 724,14, incluido el IGV.

8. CONCLUSIONES:

Considerando los requerimientos actuales y la necesidad de contar con la protección antimalware, se recomienda la contratación suscripciones de software de protección antimalware, incluyendo las actualizaciones de software y soporte técnico correspondientes por el periodo de tres (03) años.

Lima, 11 de febrero de 2019

cc.

BANCO CENTRAL DE RESERVA DEL PERÚ

FIRMADO POR:

Alexander John Anthony GAMBOA INGA
Especialista en Redes, Telecomunicaciones y Bases de Datos
Departamento de Redes, Telecomunicaciones y Bases de Datos

Leandro Manuel ALVAREZ FIGUEROA
Jefe de Departamento de Redes, Telecomunicaciones y Bases de Datos
Departamento de Redes, Telecomunicaciones y Bases de Datos

VISADO POR:

Leandro Manuel ALVAREZ FIGUEROA
Subgerente de Servicios de Tecnologías de Información Interino
Subgerencia de Servicios de Tecnologías de Información

Felipe Ernesto ROEL MONTELLANOS
Gerente de Tecnologías de Información
Gerencia de Tecnologías de Información

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