

# BANCO CENTRAL DE RESERVA DEL PERÚ

INFORME N° 0080-2022-GTI230-N

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

Lima, 25 de abril de 2022

### 1. NOMBRE DEL ÁREA:

Dpto. de Ciberseguridad y Redes

### 2. RESPONSABLE DE LA EVALUACIÓN:

Luis Alberto Peña Palacios

### 3. CARGO:

Especialista en Ciberseguridad y Redes

### 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 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 2014, el

# BANCO CENTRAL DE RESERVA DEL PERÚ

uso específico de una solución de antimalware no permitirá implementar los controles requeridos en la norma mencionada antes:

<b>Dominio</b>	<b>Sub-Dominio</b>	<b>Objetivos de control</b>	
Gestión de activos	Manejo de los medios	8.3.1	Gestión de medios removibles
Seguridad Física y ambiental	Equipos	11.2.1	Emplazamiento y protección de los equipos
		11.2.6	Seguridad de equipos y activos fuera de las instalaciones
Seguridad de las operaciones	Protección contra códigos maliciosos	12.2.1	Controles contra códigos maliciosos
	Control del Software operacional	12.5.1	Instalación de software en sistemas operacionales

## 5. ALTERNATIVAS:

Debido a que es una solución con la cual ya cuenta el BCRP desde el año 2019, y el cual ha sido solicitado sea estandarizado, lo que se desea es contratar el servicio de renovación de suscripciones.

## 6. 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 año (1) año y cinco (5) meses.
- 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.

## 7. 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 año (1) año y cinco (5) meses.

cc.

# BANCO CENTRAL DE RESERVA DEL PERÚ

FIRMADO POR:

VISADO POR: