BANCO CENTRAL DE RESERVA DEL PERÚ

MEMORANDO Nº 0276-2023-ADM110-N

A:	Javier Ernesto Olivera Vega Gerente Central de Administración
DE:	César Oscar Delizzia Infante Jefe de Departamento de Programación Logística
ASUNTO:	Estandarización de las suscripciones de software de protección antimalware marca Kaspersky.
REFERENCIA:	Informe N° 0117-2023-GTI230-N
FECHA:	03 de julio de 2023

Mediante Informe N° 0117-2023-GTI230-N el Departamento de Ciberseguridad y Redes, en calidad de área usuaria, solicita la estandarización de las suscripciones de software de protección antimalware de la marca Kaspersky para la plataforma informática del Banco Central de Reserva del Perú (BCRP).

De acuerdo con lo indicado en el mencionado informe, el BCRP cuenta en la actualidad con el servicio de detección y respuesta ante amenazas, basado en la marca Kaspersky, que contiene dentro de sus módulos a Kaspersky Endpoint Agent (KEA), que brinda la funcionalidad EDR, que son herramientas que proporcionan monitoreo y análisis continuo de los endpoint. El KEA (versión 3.13) está desplegado a nivel de estaciones y servidores con un contrato vigente hasta el 06 de julio de 2024.

Las suscripciones de software de protección antimalware permite la protección antimalware a los endpoints del BCRP donde se encuentran incluidas las estaciones y los servidores. Estas suscripciones 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 la capacidad de integración a plataformas virtuales con el hypervisor designado.

La contratación de las suscripciones de software de protección antimalware Kaspersky es complementaria con el servicio de detección y respuesta ante amenazas de Kaspersky debido a que la integración entre ambos productos permite la retroalimentación de indicadores de amenazas. Asimismo, es imprescindible que la solución antimalware sea de la marca Kaspersky para garantizar la compatibilidad con el componente KEA v 3.13 del servicio de detección y respuesta ante amenazas.

Considerando el informe elaborado por el área usuaria, la normatividad vigente y la evaluación del Departamento de Programación Logística, se concluye que procede las suscripciones de software de protección antimalware marca Kaspersky por el periodo de siete meses hasta el 05 de julio de 2024, por lo que corresponde al Gerente Central de Administración autorizar su estandarización, en cumplimiento de la delegación

dispuesta por la Gerencia General en el literal j) del numeral 10 de la Decisión de Gerencia General 0053-2018-BCRP.

La presente estandarización tendrá vigencia durante el procedimiento de selección que se lleve a cabo para las suscripciones de software de protección antimalware marca Kaspersky para la plataforma informática del BCRP.

Atentamente,

BANCO CENTRAL DE RESERVA DEL PERÚ

FIRMADO POR:

Cesar Oscar DELIZZIA INFANTE
Jefe de Departamento de Programación Logística
Departamento de Programación Logística

VISADO POR:

Jessica Judith GUEVARA PADILLA
Subgerente de Logística
Subgerencia de Logística

Jose Arturo Alberto PASTOR PORRAS
Gerente de Compras y Servicios
Gerencia de Compras y Servicios

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

BANCO CENTRAL DE RESERVA DEL PERÚ

INFORME Nº 0117-2023-GTI230-N

Informe de Estandarización - Suscripciones de Software de Protección Antimalware

1. NOMBRE DEL ÁREA:

Dpto. de Ciberseguridad y Redes

2. RESPONSABLE DE LA EVALUACIÓN:

Josue David Asurza Caceres, Especialista de Ciberseguridad
Christian Manuel Garcia Cerna, Jefe de Departamento de Ciberseguridad y Redes Interino.
Miguel Angel Tejada Malaspina, Subgerente de Servicios de Tecnologías de Información.
Marco Antonio Granadino Caceres, Subgerente de Riesgos de Tecnologías de Información.

3. DESCRIPCIÓN DEL EQUIPAMIENTO O INFRAESTRUCTURA PREEXISTENTE

El Banco cuenta en la actualidad con el servicio de Detección y Respuesta ante Amenazas, basado en la marca Kaspersky, que contiene dentro de sus módulos a Kaspersky Endpoint Agent (KEA), que brinda la funcionalidad EDR, que son herramientas que proporcionan monitoreo y análisis continuo de los endpoint. KEA (versión 3.13) está desplegado a nivel de estaciones y servidores. Dicho servicio cuenta con contrato vigente hasta el 06 de Julio de 2024.

4. DESCRIPCIÓN DEL BIEN O SERVICIO REQUERIDO

Contratación de suscripciones de software de protección antimalware para la plataforma informática del BCRP, incluyendo desktops, laptops y entornos virtuales.

5. USO O APLICACIÓN

Permitirá realizar la protección antimalware a los endpoints del Banco donde se encuentran incluidos los estaciones y servidores. 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 hypervisor designado.

Actualmente el BCRP utiliza para dichas funciones los siguientes productos:

- Kaspersky Total Security for Business
- Kaspersky Hybrid Cloud Security Server
- Kaspersky Hybrid Cloud Security Desktop

6. JUSTIFICACIÓN

6.1. Aspectos técnicos

En la actualidad el Banco utiliza una solución de protección antimalware de la marca Kaspersky conformada por los productos indicados en el numeral 5. Dichos productos son compatibles con el componente KEA (Kaspersky Endpoint Agent), versión 3.13, del servicio de Detección y Respuesta ante Amenazas, cuyo contrato es vigente hasta el 06 de Julio de 2024. El fabricante Kaspersky garantiza dicha compatibilidad solo con productos antimalware de su misma marca según se indica en los siguientes URLs:

- Información sobre KEA 3.13 y su compatibilidad con soluciones antimalware: https://support.kaspersky.com/help/KEA/3.13/en-US/193103.htm,

- Información de KATA en su versión 4.1 y su compatibilidad con soluciones antimalware: https://support.kaspersky.com/KATA/4.1/en-US/194530.htm

Nota: KATA es también un componente del servicio de detección y respuesta ante amenazas, que recibe telemetría de parte de KEA.

Es importante señalar que el período solicitado para la presente contratación es de siete (07) meses, para que la finalización de la suscripción antimalware coincida con el fin del servicio que incluye a KEA, lo que permitirá que en el 2024 se reemplacen ambas soluciones sin dependencias mutuas.

6.2. Verificación de los presupuestos

a. La Entidad posee determinado equipamiento o infraestructura pudiendo ser maquinarias, equipos, vehículos, u otro tipo de bienes, así como ciertos servicios especializados.

El Banco cuenta en la actualidad con el servicio de Detección y Respuesta ante Amenazas que contiene dentro de sus módulos a Kaspersky Endpoint Agent (KEA, actualmente en la versión 3.13) que brinda la funcionalidad EDR, que son herramientas que proporcionan monitoreo y análisis continuo de los endpoint. KEA está desplegado a nivel de estaciones y servidores.

b. Los bienes o servicios que se requiere contratar son accesorios o complementarios al equipamiento o infraestructura preexistente, e imprescindibles para garantizar la funcionalidad, operatividad o valor económico de dicho equipamiento o infraestructura.

La contratación de las suscripciones de software de protección antimalware Kaspersky **es complementaria** con el servicio de Detección y Respuesta Ante Amenazas de Kaspersky debido a que la integración entre ambos productos permite la retroalimentación de indicadores de amenazas. **Es imprescindible** que la solución antimalware sea de la marca Kaspersky para garantizar la compatibilidad con el componente KEA v 3.13 del servicio de Detección y Respuesta Ante Amenazas, tal como se indica en el numeral 6.1.

Por lo expuesto, existiría el riesgo operativo y una afectación del servicio no controlado si se utilizase una solución antimalware de una marca distinta a Kaspersky.

7. CONCLUSIONES

Por lo expuesto anteriormente y de acuerdo con la Directiva N° 004/2016-OSCE/CD, se solicita se apruebe la estandarización del software de protección antimalware de la marca Kaspersky en el proceso de contratación de suscripciones de Software de Protección Antimalware por el periodo de siete (07) meses hasta el 05 de Julio de 2024.

8. FECHA DE LA ELABORACIÓN DEL INFORME

27 de Junio del 2023

Lima, 27 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

Christian Manuel GARCIA CERNA
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.