BANCO CENTRAL DE RESERVA DEL PERÚ

MEMORANDO Nº 0098-2022-ADM110-N

A:	Javier Ernesto Olivera Vega Gerente Central de Administración
DE:	César Oscar Delizzia Infante Jefe de Departamento de Programación Logística
ASUNTO:	Estandarización del servicio para la suscripción de software de protección antimalware Kaspersky
REFERENCIA:	Informe N° 0081-2022-GTI230-N
FECHA:	26 de abril de 2022

Por medio del presente solicito a usted se sirva aprobar el Informe N° 0081-2022-GTI230-N elaborado por el Departamento de Ciberseguridad y Redes de la Subgerencia de Servicios de Tecnologías de Información, referido a la estandarización del servicio para la suscripción de software de protección antimalware Kaspersky.

De acuerdo con lo indicado en el informe, el Banco cuenta con una solución de detección y respuesta ante amenazas marca Kaspersky, conformado por:

- Kaspersky anti targeted attack platform EDR agent,
- Kaspersky managed protection for Kata+kes,
- Kaspersky maintenance service agreement for Kaspersky anti targeted attack platform y
- Kaspersky incident response latin america edition.

La renovación de las suscripciones antimalware Kaspersky es complementaria con la solución de Detección y Respuesta Ante Amenazas de Kaspersky que está instalada en todas las computadoras del Banco, porque permite la configuración las políticas y exclusiones en el Endpoint que son gestionadas desde la consola de antimalware Kaspersky. Asimismo, el requerimiento es imprescindible porque este software garantizará la operatividad de la solución Detección y Respuesta Ante Amenazas a través del uso de la consola de gestión centralizada de antimalware, debido que permite la recopilación de amenazas generadas en las computadoras del banco y centralizarlas en la consola para análisis y gestión.

El informe de la referencia se enmarca en el proceso de estandarización previsto en el numeral 29.4 del Artículo 29 del Reglamento de la Ley de Contrataciones y la Directiva N° 004-2016-OSCE/CD. La presente estandarización tendrá vigencia durante el procedimiento de selección que se lleve a cabo para la contratación del servicio para la suscripción de software de protección antimalware Kaspersky.

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:

Gustavo Alberto AMPUERO ELESPURU
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 0081-2022-GTI230-N

Informe técnico de estandarización – Suscripciones de Software de Protección Antimalware Kaspersky

Lima, 25 de abril de 2022

1. NOMBRE DEL ÁREA:

Dpto. de Ciberseguridad y Redes

2. RESPONSABLE DE LA EVALUACIÓN:

Luis Alberto Peña Palacios, Especialista en Ciberseguridad y Redes

3. DESCRIPCIÓN DEL EQUIPAMIENTO O INFRAESTRUCTURA PREEXISTENTE

El Banco cuenta en la actualidad con una solución de Detección y Respuesta ante Amenazas que contiene dentro de sus módulos el Kaspersky EDR Agent (Endpoint Detection and response, que son herramientas que proporcionan monitoreo y análisis continuo de los endpoint y la red). El Agente mencionada es desplegado a nivel de Desktop y servidores permitiendo su monitoreo y control desde la consola centralizada de Kaspersky.

Dicho modulo permite el análisis del tráfico y monitoreo de las estaciones del Banco y hace uso de la gestión de políticas realizada por el Kaspersky endpoint security (Componente antimalware de la solución) y la consola de Gestión centralizada de Kaspersky que son parte de la solución actual de antimalware desplegada en el banco.

4. DESCRIPCIÓN DEL BIEN O SERVICIO REQUERIDO

Se requiere la adquisición Kaspersky Total Security for Business (1614 nodos), Kaspersky Hybrid Cloud Security for Virtualization, Server (282 virtual servers Windows y 150 Linux), Kaspersky Hybrid Cloud Security for Virtualization, Desktop (100 virtual workstations) y la protección de 1000 casillas de correo office 365 y 100 casillas de correo micrsoft exchange on premise.

5. USO O APLICACIÓN

Permitirá realizar la protección antimalware a los endpoints del banco donde se encuentra incluidos los equipos personales, servidores y escritorios remotos. Los cuales estand desplegados en la oficina principal y las sucursales del banco. Asimismo, permitirá la gestión centralizada de las políticas de seguridad asociadas a los endpoints.

La solución permitirá la gestión de análisis, políticas y excepciones asociadas al módulo de Kaspersky EDR Agent asociado a la solución de Detección y Respuesta ante amenazas.

6. JUSTIFICACIÓN

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 una solución de Detección y Respuesta Ante Amenazas marca Kaspersky:

- Kaspersky Anti Targeted Attack Platform EDR Agent
- Kaspersky Managed Protection for KATA+KES
- Kaspersky Maintenance Service Agreement for Kaspersky Anti Targeted Attack Platform
- Kaspersky Incident Response Latin America Edition

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 renovación de las suscripciones antimalware Kaspersky **es complementaria** con la solución de Detección y Respuesta Ante Amenazas de Kaspersky que está instalada en todas las computadoras del Banco, porque permite la configuración las políticas y exclusiones en el Endpoint Detection and response que son gestionadas desde la consola de antimalware Kaspersky.
  Asimismo, el requerimiento **es imprescindible** porque este software garantizará la operatividad de la solución Detección y Respuesta Ante Amenazas a través del uso de la consola de gestión centralizada de antimalware, debido que permite la recopilación de amenazas generadas en las computadoras del banco y centralizarlas en la consola para análisis y gestión.

7. CONCLUSIONES

Por lo expuesto anteriormente y de acuerdo con la Directiva N° 004/2016-OSCE/CD, se solicita la aprobación de la estandarización para la Renovación de las suscripciones de la solución antimalware en la marca Kaspersky.

8. FECHA DE LA ELABORACIÓN DEL INFORME

Lima, 25, de abril del 2022

cc. Departamento de Programación Logística - César Oscar Delizzia Infante
Departamento de Programación Logística - Carlos Hector Galvez Valcarcel

BANCO CENTRAL DE RESERVA DEL PERÚ

FIRMADO POR:

Luis Alberto PEÑA PALACIOS
Especialista en Ciberseguridad y Redes
Departamento de Ciberseguridad y Redes

Leandro Manuel ALVAREZ FIGUEROA
Jefe de Departamento de Ciberseguridad y Redes
Departamento de Ciberseguridad y Redes

VISADO POR:

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

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

BANCO CENTRAL DE RESERVA DEL PERÚ

INFORME Nº 0127-2022-GTI230-N

Informe complementario - Estandarización para la renovación de suscripciones antimalware Kaspersky

Referencia: **INFORME 0081-2022-230GTI-N**

Lima, 15 de junio de 2022

Con respecto al informe de la referencia, se presenta información complementaria fundamentando porque es imprescindible la estandarización de la marca Kaspersky en el proceso AS 0019-2022-BCRPLIM (Contratación del servicio de suscripción de software de protección antimalware Kaspersky):

A mayor abundamiento, es imprescindible por:

a. Compatibilidad:

La solución KATA-KEDR (forma parte del servicio de Detección y Respuesta ante Amenazas) utiliza una arquitectura basada en componentes, tal como se indica en https://support.kaspersky.com/KATA/3.7.2/en-US/194604.htm.
KEA (Kaspersky Endpoint Agent) es el componente de KATA-KEDR instalado en los dispositivos finales (estaciones y servidores), y se encuentra desplegado en el Banco de manera independiente a la solución antimalware y no como un módulo de la misma.
Al respecto, la documentación del fabricante Kaspersky recomienda mantener la compatibilidad entre las versiones de KATA y KEA empleadas (https://support.kaspersky.com/KATA/3.7.2/en-US/198583.htm) para no afectar la funcionalidad del servicio de Detección y respuesta ante amenazas correspondiente al contrato N°0131-00 2020-JUR000.
Según documentación del fabricante (https://support.kaspersky.com/KATA/3.7.2/en-US/194530.htm), la compatibilidad de operación con antivirus de otras marcas es la siguiente:

Versión de KEA	Compatibilidad de operación con KEA y número de productos antimalware de terceros
3.10	6
3.11	1
3.12	0

Al respecto, según el numeral 4 del capítulo III de la sección especifica de las bases integradas del contrato vigente correspondiente al servicio de Detección y Respuesta ante Amenazas (contrato N°0131-00 2020-JUR000), el contratista tiene la obligación de proporcionar al Banco las actualizaciones del software Kaspersky provisto como parte del servicio, del cual actualmente el Banco viene utilizando las versiones KATA 3.7.2 y KEA 3.10. Por lo que en cumplimiento de dicha obligación está en proceso la actualización de versiones de software hacia KATA 4.0 y KEA 3.12, que incluyen nuevas funcionalidades para respuesta ante amenazas avanzadas (https://support.kaspersky.com/KATA/4.0/en-US/194460.htm).
De lo indicado en el cuadro, no se puede utilizar productos antimalware de terceros con la versión de KEA 3.12, por la incompatibilidad entre los mismos,

teniendo riesgo de afectar la operación del servicio de Detección y respuesta ante amenazas.

b. Integración:
Siendo la consola de gestión (KSC - Kaspersky Security Center) imprescindible debido a que:

21) Centraliza el despliegue, permite la configuración de las políticas de administración y exclusiones en los dispositivos finales de:
- Las soluciones antimalware de Kaspersky.
- KATA-KEDR (que forma parte del servicio de Detección y Respuesta ante Amenazas) de Kaspersky.

22) La postura de ciberseguridad que mantiene el Banco a nivel de dispositivos finales es la siguiente:
- Primera capa: Antimalware, el cual realiza el bloqueo de amenazas conocidas.
- Segunda capa: La solución KATA-KEDR (parte del servicio de Detección y Respuesta ante Amenazas), la cual realiza la detección y respuesta ante amenazas desconocidas que superaron al antimalware.

KATA-KEDR retroalimenta la información de indicadores de amenazas (IoA) detectadas hacia la nube de inteligencia del fabricante (KSN - Kaspersky Security Network). Las soluciones antimalware de Kaspersky se alimentan de información de KSN (a la que accede a través de la consola de gestión KSC) y con ello puede realizar el bloqueo de estas nuevas amenazas en la primera capa.

La integración entre KATA-KEDR y las soluciones antimalware de Kaspersky desplegadas en el Banco no es posible con soluciones antimalware de otras marcas.

Por los motivos expuestos se concluye que es imprescindible la estandarización de la marca Kaspersky en el proceso AS 0019-2022-BCRPLIM (Contratación del servicio de suscripción de software de protección antimalware Kaspersky) en cumplimiento a lo establecido en el numeral 7.3 de la Directiva N° 004-2016-OSCE-CD.

cc.

BANCO CENTRAL DE RESERVA DEL PERÚ

FIRMADO POR:

Luis Alberto PEÑA PALACIOS
Especialista en Ciberseguridad y Redes
Departamento de Ciberseguridad y Redes

Leandro Manuel ALVAREZ FIGUEROA
Jefe de Departamento de Ciberseguridad y Redes
Departamento de Ciberseguridad y Redes

VISADO POR:

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

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