BANCO CENTRAL DE RESERVA DEL PERÚ

MEMORANDO Nº 0241-2024-ADM110-N

A:	Javier Ernesto Olivera Vega Gerente Central de Administración
DE:	César Oscar Delizzia Infante Jefe de Departamento de Programación Logística
ASUNTO:	Estandarización para la contratación de los servicios de soporte técnico, mantenimiento y suscripciones para prevención y control de amenazas, para la solución firewall de nueva generación (NGFW) del BCRP de la marca Palo Alto brindado por un proveedor autorizado por la marca.
REFERENCIA:	Informe Nº 0014-2024-GTI420-N
FECHA:	06 de junio de 2024

Mediante informe N° 0014-2024-GTI420-N la Subgerencia de Ciberseguridad, en calidad de área técnica, solicita la estandarización para la contratación de los servicios de soporte técnico, mantenimiento y suscripciones para prevención y control de amenazas, para la solución firewall de nueva generación (NGFW) del BCRP de la marca Palo Alto brindado por un proveedor autorizado por la marca.

De acuerdo con lo indicado en el informe, el Banco cuenta con una solución de NGFW de la marca Palo Alto. Los servicios de soporte técnico, mantenimiento y suscripciones de prevención y control de amenazas son complementarios al equipamiento preexistente. Asimismo, el requerimiento es imprescindible para garantizar la funcionalidad de la solución, manteniendo las medidas de seguridad implementadas y fortalecer el nivel de protección de la infraestructura del Banco. Al ser brindado por un proveedor autorizado por la marca, permitirá disponer de la garantía del hardware sobre los equipos físicos, actualizaciones de software (incluyendo nuevas versiones y parches), soporte técnico del fabricante y local, así como suscripciones para prevención y control de amenazas que brinden un adecuado nivel de protección a la red informática.

Considerando el informe elaborado por el área técnica, la normatividad vigente y la evaluación del Departamento de Programación Logística, se concluye que procede la estandarización para la contratación de los servicios de soporte técnico, mantenimiento y suscripciones para prevención y control de amenazas, para la solución firewall de nueva generación (NGFW) del BCRP de la marca Palo Alto brindado por un proveedor autorizado por la marca, 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 proceso de selección que se lleve a cabo para la contratación de los servicios de soporte técnico, mantenimiento y suscripciones para prevención y control de amenazas, para la solución firewall de nueva generación (NGFW) del BCRP de la marca Palo Alto brindado por un proveedor autorizado por la marca.

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

Nº Sistema: MEM-2024-004564
Firmado con certificados digitales emitidos por RENIEC. Los nombres de los firmantes figuran en la última página.

BANCO CENTRAL DE RESERVA DEL PERÚ

INFORME Nº 0014-2024-GTI420-N

Estandarización - Contratación de los servicios de soporte técnico, mantenimiento y suscripciones para prevención y control de amenazas, para la solución firewall de nueva generación (NGFW) del BCRP de la marca Palo Alto brindado por un proveedor autorizado por la marca

---

1. NOMBRE DEL ÁREA

Subgerencia de Ciberseguridad

2. RESPONSABLES DE LA EVALUACIÓN Y CARGOS

Marco Granadino Cáceres, Subgerente de Ciberseguridad
Alexander Gamboa Inga, Jefe de Departamento de Seguridad Informática Interino
Carlos Ivan Sulca Galarza, Especialista en Seguridad Informática

3. DESCRIPCIÓN DEL EQUIPAMIENTO O INFRAESTRUCTURA PREEXISTENTE

El Banco cuenta en la actualidad con una solución de NGFW de la marca Palo Alto, conformada por:

- ✓ Dos (02) appliance físicos PA 3250, en una configuración de alta disponibilidad activo/standby.
- ✓ Licenciamiento perpetuo para virtualización de firewalls en los appliances físicos (permite como máximo 6 virtual systems en cada firewall).
- ✓ Suscripciones de Prevención y control de amenazas.
- ✓ Un (01) appliance físico PA 3250 con el rol de cold spare, de forma que pueda cubrirse inmediatamente la falla de alguno de los appliances que se encuentran operando.
- ✓ Un (01) appliance virtual Panorama, para permitir la administración centralizada de los NGFW, así como registro y almacenamiento de eventos. Este componente cuenta con licencia perpetua para la gestión de 25 dispositivos.

4. DESCRIPCIÓN DEL BIEN O SERVICIO REQUERIDO

Se requiere la contratación por el periodo de tres (03) años de los servicios de soporte técnico, mantenimiento y suscripciones para prevención y control de amenazas para la solución de firewall de nueva generación (NGFW) del BCRP de la marca Palo Alto, brindado por un proveedor autorizado por la marca.

El servicio consiste en lo siguiente:

- ✓ Garantía de hardware
- ✓ Actualizaciones de software
- ✓ Soporte técnico del fabricante (escalamiento)
- ✓ Suscripciones para prevención y control de amenazas
- ✓ Servicio de mesa de ayuda y soporte técnico local 24 x 7
- ✓ Servicio de mantenimiento técnico preventivo.

5. USO O APLICACIÓN QUE SE DARÁ AL BIEN O SERVICIO REQUERIDO

El servicio de soporte técnico, mantenimiento y suscripciones para la prevención y control de amenazas para la solución firewall de nueva generación (NGFW) del BCRP de la marca Palo Alto, estará conformado con las siguientes características que beneficiarán al BCRP:

- ✓ **Garantía de hardware**
  Reemplazo de piezas o del equipamiento total por fallas del hardware (RMA).

- ✓ **Actualizaciones de software**: Acceso a versiones nuevas del software utilizado en los equipos, así como a correcciones (parches, hotfixes).

- ✓ **Soporte técnico del fabricante (escalamiento)**
  Permite el escalamiento de casos de soporte técnico para su atención por el TAC (Technical Assistance Center) del fabricante.

- ✓ **Suscripciones para prevención y control de amenazas**
  Permite la protección de una nueva generación de amenazas (malware avanzado, botnets, APTs), así como protección de tráfico DNS y filtrado URL a través de las siguientes suscripciones:

  - IPS, antivirus y protección contra bots.
  - Sandboxing on cloud.
  - Protección de tráfico DNS.
  - Filtro avanzado de URLs.

- ✓ **Servicio de mesa de ayuda y soporte técnico local 24 x 7**: Asignación de tickets ante incidentes, atención de soporte técnico especializado (incluso en forma local).

- ✓ **Servicio de mantenimiento técnico preventivo**: Mantenimientos técnicos preventivos periódicos (mínimo semestral).

6. JUSTIFICACIÓN

A continuación, se sustentan los requisitos para proceder a la estandarización:

6.1. ASPECTOS TÉCNICOS

Los firewalls son elementos imprescindibles en toda arquitectura de ciberseguridad, dadas sus capacidades de proporcionar control sobre las conexiones de red a través la segmentación en zonas de seguridad, permitiendo sólo tráfico autorizado y bloqueando tráfico malicioso. Sus funcionalidades han evolucionado en el tiempo y actualmente disponemos de las soluciones del tipo Next Generation Firewall (NGFW) que incorporan las siguientes capacidades:

- ✓ <u>Inspección en la capa de aplicación</u>
  Proporciona visibilidad y control completo a nivel de aplicaciones, a través de la inspección su comportamiento y la interacción que tienen con los usuarios. No sólo se requiere identificar correctamente las

aplicaciones, sino que también deben identificar correctamente las variables de su uso contextual, para poder tomar acciones apropiadas, más allá de sólo permitir/denegar.

- ✓ Next Generation IPS
  Los sistemas IPS detectan y bloquean ataques enfocándose en vulnerabilidades de sistemas y aplicaciones, para ello cuentan con la capacidad de decodificar protocolos y detectar patrones de tráfico (signatures). Los IPS tradicionales por lo general utilizan puerto y protocolo como primer método de clasificación de tráfico, motivo por el cual son susceptibles a errores ante las técnicas de evasión modernas. La tecnología NGFW incluye un módulo IPS que aprovecha las capacidades de identificación de aplicaciones, para una operación eficiente y coordinada.

- ✓ Uso de inteligencia basada en nube
  NGFW permite utilizar la nube como fuente de información dinámica para el bloqueo de atacantes que estén siendo detectados en base a su comportamiento en Internet, permitiendo también contar con información de geolocalización y de actividad sospechosa a nivel mundial.

- ✓ Sandboxing
  Permite la ejecución en entornos aislados (sandbox), de procesos sospechosos para determinar sus posibles efectos. El sandbox puede ubicarse en forma local en la red interna (on premise) o emplear un servicio en la nube (on cloud).

Las funcionalidades mencionadas son generalmente ofertadas bajo la modalidad de servicios que se habilitan en la infraestructura utilizada por la solución NGFW. Asimismo, para una óptima operación, se utiliza plataforma appliance (hardware y software de propósito específico).

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 una solución de NGFW marca Palo Alto, cuyos componentes se detallan en el numeral 3.

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 preexistente.

Los servicios de soporte técnico, mantenimiento y suscripciones de prevención y control de amenazas **son complementarios** a la solución NGFW del BCRP, conformada por equipos físicos y virtuales de la marca Palo Alto. Asimismo, **son imprescindibles** para garantizar la funcionalidad de la solución NGFW, manteniendo las medidas de

seguridad implementadas y fortalecer el nivel de protección de la infraestructura del Banco (acceso a SWIFT, sistema LBTR, portal web institucional, acceso Wireless, entre otros). Al ser brindado por un proveedor autorizado por la marca, permitirá disponer de la garantía del hardware sobre los equipos físicos, actualizaciones de software (incluyendo nuevas versiones y parches), soporte técnico del fabricante y local, ante posibles incidencias que puedan presentarse con el uso de la solución, así como suscripciones para prevención y control de amenazas, que brinden un adecuado nivel de protección a la red informática institucional.

Debemos considerar que el software de gestión centralizada Panorama es utilizado para la administración de los firewalls de Lima y Sucursales (Contratos N° 0058-00 2021-JUR000, de la Oficina Principal; N° 0020-00 2022-JUR000, de las sucursales; y N° 0142-00 2024-JUR000, del Centro Externo de Respaldo Piura), los cuales son de la marca Palo Alto. Panorama no puede ser reemplazado por un software similar de otra marca, pues se requiere compatibilidad completa para garantizar su operatividad con los Firewalls con que ya cuenta el BCRP.

6.3. Incidencia Económica de la Contratación

Realizar la contratación del soporte técnico, mantenimiento y suscripciones para prevención y control de amenazas para la solución de firewall de nueva generación (NGFW) del BCRP, de la marca Palo Alto, brindada por un proveedor autorizado por la marca, incidirá favorablemente en la puesta en valor de los bienes preexistentes, permitiendo además la protección de la red informática institucional. La implementación de otra solución implicaría un nuevo proyecto de largo alcance que impactaría en términos de tiempo y costos adicionales para su implementación.

7. CONCLUSIONES

En cumplimiento con lo establecido en la Directiva N°004-2016-OSCE/CD que norma la estandarización, se solicita se apruebe la estandarización de la contratación de los servicios de soporte técnico, mantenimiento y suscripciones para prevención y control de amenazas, para la solución de firewall de nueva generación (NGFW) del BCRP de la marca Palo Alto, brindado por un proveedor autorizado por la marca.

Lima, 29 de mayo de 2024

cc.

BANCO CENTRAL DE RESERVA DEL PERÚ

FIRMADO POR:

Carlos Ivan SULCA GALARZA
Especialista en Seguridad Informática
Departamento de Seguridad Informática

Alexander John Anthony GAMBOA INGA
Jefe del Departamento de Seguridad Informática (i)
Interino
Departamento de Seguridad Informática
Firma como encargado.

Marco Antonio GRANADINO CACERES
Subgerente de Ciberseguridad
Subgerencia de Ciberseguridad

Silvia Elizabeth MEDINA MORENO
Gerente de Tecnologías de Información
Gerencia de Tecnologías de Información

VISADO POR: