

# BANCO CENTRAL DE RESERVA DEL PERÚ

INFORME N° 0214-2022-GTI230-N

*Informe técnico previo de evaluación de software - Servicio de contratación de suscripciones de la solución de seguridad informática para el correo electrónico*

Lima, 22 de septiembre 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:**

El correo electrónico se ha convertido en uno de los principales medios de comunicación, su bajo costo, facilidad de uso y alta difusión han contribuido a ello. Sin embargo, estos mismos factores han hecho de él, uno de los elementos más vulnerables de la infraestructura de red, convirtiéndose en vía de ingreso de mensajes no solicitados (spam) y mensajes de contenido fraudulento (phishing), ambos con objetivos tales como ocasionar fraudes, robo de identidad, liberación de malware dentro de las empresas y daño en la disponibilidad de los servicios.

Ante esta situación se desarrollaron sistemas de protección que han evolucionado a través de los años, desde un gateway (mail relay) con análisis de contenido y antimalware, hasta los modernos sistemas ESG (Email Security Gateway) con tecnología de filtro de reputación, protección contra ataques de rebote (bounce attacks) y mecanismos de autenticación de transmisión.

En el año 2008 el BCRP adquirió suscripciones para una solución ESG, denominada Cisco Ironport, durante los años siguientes se amplió y renovó la cobertura de dicha solución. En el año 2016 la plataforma de protección se migró hacia appliances virtuales ESA (Email Security Appliance) del modelo Cisco C300V y se amplió la cobertura a 1250 casillas de correo electrónico. Posteriormente, en el año 2018 se incorporó un appliance virtual SMA (Security Management Appliance) del modelo Cisco M300V, encargado de la centralización de cuarentenas y tracking de mensajes de correo electrónico de los appliances Cisco C300V, en el 2019 se renovó el servicio de los 2 appliances M300V y el appliance C300V.

A continuación, se presenta un resumen de los servicios proporcionados por la solución:

- Incluye el servicio de filtro de reputación, con actualización continua por parte del fabricante, que permite bloquear amenazas en forma proactiva.
- Utiliza un motor antimalware (Sophos) diferente del que emplean los nodos finales (Kaspersky) con lo que proporciona protección adicional.

## BANCO CENTRAL DE RESERVA DEL PERÚ

- Incluye un mecanismo proactivo de detección de malware basado en tendencias (Virus Outbreak Filters).
- Cuenta con protección contra bounce attacks.
- Gestión centralizada de reportes, cuarentenas y el seguimiento (tracking) del flujo de mensajes de correo electrónico.

### 5. ALTERNATIVAS:

De la revisión de información relevante en estudios actuales sobre las mejores soluciones de Email Security existentes, tales como el análisis de sites como Gartner, Forrester o Radicati hemos podido verificar distintas alternativas de solución que cumplan con los requerimientos similares o superiores a la solución actual de estas opciones se analizó las siguientes:

- Proofpoint Email Protection Suite – Proofpoint.
- Cisco Secure Email – Cisco

### 6. ANÁLISIS COMPARATIVO TÉCNICO:

De las alternativas mencionadas en el punto anterior se comparó las funciones requeridas por el banco para la protección de nuestro servicio de correos y verificó que ambas soluciones cuentan con las funcionalidades, como se menciona en el cuadro anterior:

|                                   | Proofpoint Email Protection Suite | Cisco Secure Email |
|-----------------------------------|-----------------------------------|--------------------|
| Filtro reputacional de remitentes | Sí                                | Sí                 |
| Motor Antimalware interno         | Sí                                | Sí                 |
| Detección de malware              | Sí                                | Sí                 |
| Gestión centralizada              | Sí                                | Sí                 |
| Límites de volumen de envíos      | Sí                                | Sí                 |
| Protección contra bounce attacks  | Sí                                | Sí                 |

Además de cumplir con los requisitos de la necesidad del banco, ambas soluciones se encuentran muy bien posicionados dentro de los rankings de análisis de las empresas de benchmarking mencionadas en el punto anterior, lo que nos brinda un mayor respaldo para la utilización de las mismas en un tema tan crítico como es hoy en día la seguridad de del Email corporativo.

### 7. ANÁLISIS COMPARATIVO DE COSTO – BENEFICIO:

#### Beneficios:

- Protección antispam y antimalware en el gateway de correo electrónico (mail relay).
- Configuración en alta disponibilidad, que permite mantener la continuidad del servicio aún ante el evento de caída del site principal.
- Consola de web para gestión centralizada de reportes, cuarentenas y el seguimiento (tracking) del flujo de mensajes de correo electrónico

#### Costos:

## **BANCO CENTRAL DE RESERVA DEL PERÚ**

- Suscripción a los servicios del fabricante
- Actualizaciones de software (incluyendo el suministro de nuevas versiones y patches), soporte técnico del fabricante (escalamiento), por el periodo de un (01) año.
- 
- Servicios del partner (proveedor local)
- Mesa de ayuda y soporte presencial, en el esquema 24x7x2 y mantenimiento técnico preventivo anual.

En lo que respecta a los costos asociados se estima que el costo debe estar alrededor de S/ 160 000,00 incluido IGV.

### **8. CONCLUSIONES:**

Por lo expuesto anteriormente, se considera conveniente la contratación del servicio de suscripciones para la solución de seguridad informática para el correo electrónico, por el periodo de un (01) año.

**cc.**

# **BANCO CENTRAL DE RESERVA DEL PERÚ**

FIRMADO POR:

VISADO POR: