BANCO CENTRAL DE RESERVA DEL PERÚ

INFORME Nº 0104-2023-GTI230-N

Informe técnico previo de evaluación de software - Contratación de suscripciones de seguridad informática para el correo electrónico (antispam)

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 ido evolucionando 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.

Hoy en día con la tendencia creciente de las soluciones en nube, es un factor para considerar las ventajas que nos brinda este tipo de implementaciones entre las que podemos considerar la disponibilidad que se tiene al tener el servicio en un tenant ajeno a los datacenter de nuestra entidad. A esto podemos sumar el ahorro en los recursos que son necesarios para implementar una solución on premise.

Es necesario considerar que actualmente el banco cuenta con una solución hibrida para su servicio de correos, teniendo el mayor volumen de los buzones alojados en el tenant de Office 365 y manteniendo cuentas genéricas en la solución on premise de Exchange, por lo que la solución a considerar debe tener la integración con ambas soluciones de correo.

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

- Incluye el servicio de filtro de reputación, con actualización continua por parte del fabricante, que permite bloquear amenazas en forma proactiva.
- Contar con protección antimalware para el correo electrónico.
- Incluye un mecanismo proactivo de detección de malware basado en tendencias.

- Cuenta con protección contra bounce attacks.
- Gestión centralizada de reportes, cuarentenas y el seguimiento (tracking) del flujo de mensajes de correo electrónico.

5. ALTERNATIVAS:

En el mercado nacional hemos identificado las siguientes soluciones de seguridad, las mismas que están también consideradas en las evaluaciones de empresas consultoras de prestigio (Gartner, Forrester, Radicatti):

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

6. ANÁLISIS COMPARATIVO TÉCNICO:

El análisis técnico ha sido realizado de conformidad con la metodología establecida en el documento "Guía Técnica sobre evaluación de software en la administración pública" (Resolución Ministerial N° 139-2004-PCM), tal como se exige en el reglamento de la Ley N° 28612.

Propósito de evaluación
Comparar alternativas de productos existentes en el mercado.

Identificar el tipo de producto
Solución de control de acceso a red.

Identificación del modelo de calidad
Se aplicará el Modelo de Calidad de Software descrito en la Parte I de la Guía de evaluación de software aprobado por RM N° 139-2004-PCM.

Selección de métricas.
Las métricas fueron seleccionadas en base a las características técnicas descritas en el Anexo N° 1.

7. ANÁLISIS COMPARATIVO DE COSTO – BENEFICIO:

Teniendo en que actualmente el Banco cuenta con el servicio de correos en Office 365, se optó por analizar nuevas soluciones en nube que nos permitan una integración hibrida, a la altura de los requerimientos actuales que tiene el banco y que nos permite hacer frente a la creciente amenaza de correos maliciosos.

Entre los beneficios que nos brinda un servicio de suscripciones en nube tenemos lo siguiente:

- Al ser suscripciones en nube el Banco no tiene que brindar recursos tecnológicos para soportar las herramientas que forman parte del servicio.
- Una de las cosas más importantes para tener en cuenta al elegir entre soluciones basadas en la nube es la alta disponibilidad. El servicio de antispam estará habilitado incluso si no se encuentran disponibles los datacenter del Banco.
- Hoy en día se tiene reportes continuos de vulnerabilidades que afectan distintas soluciones de seguridad, lo que conlleva a despliegue de parches y/o actualizaciones para cubrir dichas vulnerabilidades. En una solución on premise esto se ve reflejado en ventanas de trabajo especiales para el despliegue que

interrumpen el servicio, mientras que en un servicio en la nube estos parches son ejecutados por el SSP (Security Service Provider) sin interrumpir el servicio que se brinda al Banco.
- El servicio en nube nos brinda mayor capacidad de escalamiento en caso sea necesario, ya que no implica aumento de recursos virtuales o físicos brindados por el Banco.
- En los servicios en nube se tiene menores tiempos de implementación dado que son suscripciones en una plataforma contratada y no es necesario proporcionar recursos de hardware on premise.
- El uso de un servicio de seguridad informática para el correo se ve reflejado en un menor consumo del ancho de banda para el Banco.

Costos:

Las prestaciones requeridas corresponden al periodo de tres (03) años de servicio e incluyen lo siguiente:

- Prestación Principal: Suscripción a los servicios del fabricante
  Se recomienda la contratación de las suscripciones del servicio de antispam por un periodo de 3 años.

- Prestación accesoria: Servicios del partner (proveedor local)
  Mesa de ayuda y soporte presencial, en el esquema 24x7 y mantenimiento técnico preventivo anual.

En base a las cotizaciones referenciales obtenidas se estima que el costo del servicio se encuentra dentro del margen presupuestado en PAC 2023.

8. CONCLUSIONES:

Por lo expuesto anteriormente, se considera conveniente la Contratación de suscripciones de seguridad informática para el correo electrónico (antispam), por el periodo de tres (03) años.

BANCO CENTRAL DE RESERVA DEL PERÚ

Anexo 1

Atributos	Puntaje Maximo	Proofpoint Email Protection Suite	Cisco Secure Email
Filtro reputacional de remitentes	20	20	20
Motor Antimalware interno	20	19	18
Detección de malware	20	19	19
Gestión centralizada	10	9	8
Límites de volumen de envíos	15	15	15
Protección contra bounce attacks	15	13	13
Total	100	95	93

Lima, 5 de junio de 2023

cc.

BANCO CENTRAL DE RESERVA DEL PERÚ

FIRMADO POR:

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

Alexander John Anthony GAMBOA INGA
Jefe de Departamento de Ciberseguridad y Redes Interino
Departamento de Ciberseguridad y Redes
Firma como encargado.

VISADO POR:

Luis Enrique DIAZ VARGAS
Subgerente de Servicios de Tecnologías de Información Interino
Subgerencia de Servicios de Tecnologías de Información
Firma como encargado.

Marco Antonio GRANADINO CACERES
Subgerente de Riesgos de Tecnologías de Información
Subgerencia de Riesgos de Tecnologías de Información

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

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