

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”  
“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración  
de las heroicas batallas de Junín y Ayacucho”

CUT: 186755-2024

## **INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE N° 0001-2024-ANA- DSNIRH/AALR**

### **1. NOMBRE DEL ÁREA:**

Dirección del Sistema Nacional de Información de Recursos Hídricos

### **2. RESPONSABLE DE LA EVALUACIÓN:**

Nombre: Alberto Adrián Loza Romero

Coordinador

Coordinación de infraestructura, comunicaciones y soporte IT

Ing. Ismael Edwin Salazar Villavicencio

Director

Dirección del Sistema Nacional de Información de Recursos Hídricos

### **3. FECHA:**

17 de septiembre de 2024

### **4. JUSTIFICACIÓN:**

La Autoridad Nacional del Agua (ANA) requiere mejorar su solución actual de protección de correo electrónico para salvaguardar la información crítica de la ANA, garantizando su confidencialidad, integridad y disponibilidad.

La creciente amenaza cibernética sobre plataformas de correos electrónicos corporativas e institucionales a través de la generación masiva y sistemática de correos electrónicos no deseados (SPAM), ataques de suplantación de identidad, secuestro de credenciales a través de técnicas de correo Phishing y Spear Phishing, archivos infectados con virus informáticos, sumado a las posibles afectaciones de disponibilidad que sufren eventualmente proveedores de plataformas de colaboración y correo electrónico como el reciente caso de Microsoft el pasado 19 de julio de 2024, el cual tuvo una repercusión mundial ([https://es.wikipedia.org/wiki/Incidente\\_de\\_CrowdStrike\\_de\\_2024](https://es.wikipedia.org/wiki/Incidente_de_CrowdStrike_de_2024)); hace necesaria la adquisición de una solución líder en el mercado que reduzca o mitigue estos riesgos cibernéticos.

La adquisición de una solución Antispam líder en el mercado mejorará significativamente la seguridad, previniendo infecciones de virus informáticos y protegiendo contra correos no deseados, publicidad engañosa y enlaces maliciosos.

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”  
“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”

Actualmente, la ANA utiliza el producto de Spam and Malware Protection del fabricante Hornet Security, cuya vigencia expira el 18 de noviembre de 2024. **ES URGENTE Y NECESARIO CONTAR CON UNA NUEVA** solución de protección y mitigación de riesgos para la seguridad del correo electrónico de la ANA, que sea **SUPERIOR A LA ACTUAL** adicionando capacidades seguimiento de correo electrónico en tiempo real, control total del contenido del correo para evitar se incruste código malicioso, cifrado global S/MIME y PGP, control de políticas de cifrado seguro, sistema de archivado de correo electrónico con retención de correo electrónico durante el tiempo que se suscriba la plataforma, disponibilidad del servicio garantizada sobre el 99.9%, capacidades de realizar análisis forenses que permitan determinar el origen técnico de las amenazas, tecnologías integradas de sandbox para ATP y capacidades de supervisión y gestión DMARC 24/7 imposibilitando la suplantación de identidad a través de un control completo sobre sus protocolos de autenticación de correo electrónico.

Es de vital importancia que la tecnología propuesta se posicione como líder en el mercado y cuente con la infraestructura necesaria para garantizar la seguridad y disponibilidad del servicio de correo electrónico en la institución.

En cumplimiento de la Ley 28612, "Ley que norma el uso, adquisición y adecuación del software de la Administración Pública", se procede a evaluar el software Antispam que mejor se adapte a las necesidades de la institución.

## 5. ALTERNATIVAS DE EVALUACIÓN:

Considerando las necesidades mencionadas, se evaluará software con soporte local que cumpla con requisitos de implementación similares y que sean líderes en el Cuadrante Mágico de Gartner y/o Forrester Wave y/o IDC MarketScape para garantizar experiencia y trayectoria en el mercado. Las alternativas de solución son:

PRODUCTO EVALUADO	
FABRICANTE	PRODUCTO
CISCO	SECURE EMAIL CLOUD GATEWAY
SOPHOS	CENTRAL EMAIL ADVANCED

La información para la evaluación técnica y la elaboración de los términos de referencia se obtuvo de las páginas web de los fabricantes.

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”  
 “Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”

## 6. ANÁLISIS COMPARATIVO TÉCNICO:

El análisis técnico se basa en la metodología de la "Guía Técnica sobre evaluación de software en la administración pública" (R.M. N° 139-2004- PCM) y la Ley N.º 28612.

### 6.1. PROPÓSITO DE EVALUACIÓN:

Confirmar que las alternativas seleccionadas son las más adecuadas para satisfacer las necesidades de la ANA en cuanto a protección y mitigación de riesgos de seguridad del correo electrónico.

Determinar los atributos o características esenciales para el producto final.

### 6.2. IDENTIFICAR EL TIPO DE PRODUCTO:

Software Antispam que proteja los correos electrónicos institucionales de los profesionales de la ANA.

### 6.3. IDENTIFICACIÓN DEL MODELO DE CALIDAD:

Se aplicará el modelo de calidad de la parte I de la Guía de evaluación de software (R.M. N° 139- 2014-PCM) y la Ley N° 28612.

### 6.4. SELECCIÓN DE MÉTRICAS:

Las métricas se eligieron según las características principales de los productos a evaluar:

## MÉTRICAS: ATRIBUTOS DE LICENCIA – PLATAFORMA TECNOLÓGICA:

N°	ATRIBUTO	DESCRIPCIÓN	PUNTAJE MÁXIMO	PUNTAJE MÍNIMO	SOPHOS	CISCO
1	Integración con API de Microsoft 365	La integración a nivel de API permite que la velocidad de análisis, gestión y protección se realicen de forma más eficiente contrario a como se tiene actualmente que solo se configura través de la redirección a nivel de MX.	10	0	10	7
2	Detección de amenazas avanzadas	Permite la detección e identificación de correos electrónicos anómalos de mala intención a través de la combinación de tecnologías de Sandboxing y XDR aplicadas al correo	10	0	5	7

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”  
 “Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”

3	Soporte de protocolo SNMP y Conector SIEM	Capacidad de integrarse con sistemas de monitoreo de red mediante SNMP y conector SIEM que permita ingerir los eventos de seguridad a plataforma SIEM y EDR	10	0	8	10
4	Reconocimiento de Spam, Phishing y Spear Phishing Asistido con inteligencia artificial	Reconocimiento Spam, Phishing y Spear Phishing avanzado con capacidad de reconocimiento de múltiples idiomas, reconociendo la ubicación del ataque a través de informes de análisis forense	10	0	10	10
5	Continuidad del negocio y recuperación	Integración de capacidades de archivamiento reteniendo información por todo el tiempo que se tenga suscrita la plataforma y agregando capacidades de continuidad del negocio recibiendo y enviando correos hasta por 90 días de manera autónoma.	10	0	7	9
6	Mitigación de suplantación de identidad a través de la supervisión DMARC 24/7 y monitoreo constante de robo de credenciales en darkweb	Capacidades de rastrear fuentes de envío maliciosas y analizar DMARC presentando una gama de informes, análisis y supervisión en la plataforma, ofreciendo un control completo sobre los protocolos de autenticación de correo electrónico.	10	0	8	9
<b>TOTAL</b>			60	0	48	52

*Cuadro N° 01 – Atributos de licencia*

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”  
 “Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”

### MÉTRICAS: ATRIBUTOS DE USO

N	ATRIBUTO	DESCRIPCIÓN	PUNTAJE MÁXIMO	PUNTAJE MÍNIMO	SOPHOS	CISCO
1	Consultas y reportes	Incluye generación de consultas y actividad por usuario, dominio, gestión y exportación de reportes con análisis forense y resultados de explotación de archivos en un entorno controlado	10	0	9	10
2	Soporte	Se dispone de especialistas calificados para la instalación y configuración	10	0	10	10
3	Eficacia	Identifica la mensajería no deseada, maliciosa y otras con disponibilidad del servicio al 99.9%	10	0	9	10
4	Facilidad de uso	El usuario interactúa con familiaridad sobre la plataforma	10	0	10	8
<b>SUBTOTAL</b>			40	0	39	37
<b>TOTAL</b>			<b>100</b>	<b>0</b>	<b>86</b>	<b>90</b>

Cuadro N° 02 – Atributos de uso

### ESCALA DE MÉTRICAS:

ESCALA	DESCRIPCIÓN
2	Deficiente: La tecnología empleada no funciona correctamente y existen reportes de problemas por los usuarios
4	Regular: Tecnología con algunas limitaciones en las características
6	Bueno: Tecnología con algunas limitaciones en desempeño y funcionalidad
8	Muy Bueno: Tecnología con buen desempeño y funcionalidad
10	Excelente: Tecnología de gran desempeño y funcionalidad aprobada a nivel mundial

Cuadro N° 03 – Escala de métricas



PERÚ

Ministerio de Desarrollo Agrario y Riego

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”  
“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”

Del CUADRO N°1, se muestra los resultados de evaluación de los productos considerados para la adquisición de software ANTISPAM, en la que **SOPHOS** resulta el más adecuado para los fines de la Entidad, seguido de **CISCO**.

### 6.5. ANÁLISIS COMPARATIVO TÉCNICO/FUNCIONAL:

El análisis se realizó acorde al alcance y características generales que los fabricantes de software Antispam evaluados deben brindar:

ATRIBUTOS/CARACTERITICAS	SOPHOS	CISCO
Protege correos de dominios externos y ajenos a la empresa	SI	SI
Tiene motores para la detección de malware con la capacidad de identificar Exploits en documentos y archivos de Office	SI	SI
Incluye antimalware para análisis de amenazas desconocidas y ataques de día cero	SI	SI
Ofrece disponibilidad del servicio de protección superior a >99.8%	SI	SI
Permite mostrar distintos gráficos para dar seguimiento al tráfico de correo y cuarentenas	SI	SI
Provee autorización o denegación de correos basados en diferentes criterios de evaluación del mensaje	SI	SI
Bloqueo de palabras clave	SI	SI
Instalación en ambiente de servidores virtualizados y nube	SI	SI
Incluye tecnología de análisis sobre amenazas avanzadas basadas en Sandboxing y XDR para emails	NO	SI
Incluye funcionalidades avanzadas para la disponibilidad del correo electrónico a un 99.9%	NO	SI

Cuadro N° 04 – Análisis comparativo técnico/funcional

Se ha observado que en la evaluación que por lo menos DOS (02) soluciones cumplen con los requerimientos técnico funcional que se requiere en la Entidad.



“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”  
 “Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”

## 7. ANÁLISIS COMPARATIVO DE COSTO-BENEFICIO:

Análisis Costo – Beneficio de licencias, implementación, actualización, soporte y mantenimiento por 01 año para 2000 buzones de correo electrónico, tomado a través de proveedores locales:

SOFTWARE	COSTO	VALORACIÓN TÉCNICA	VALOR COSTO-BENEFICIO
SOPHOS	S/ 306,000.00 inc. IGV	92	3.01
CISCO	S/ 334,000.00 inc. IGV	95	2.84

*Cuadro N° 05 – Análisis costo-beneficio*

### NOTA:

- Las cotizaciones de referencia se adjuntan al presente en los Anexos.
- No se ha considerado los costos de hardware adicional, ya que la Entidad cuenta con el hardware necesario para la ejecución del software.
- Asimismo, no se han considerados los costos del soporte y mantenimiento, el personal y mantenimiento interno y la valoración de capacitación, ya que están contemplados dentro del costo de licenciamiento.
- Fórmula utilizada para el cálculo del costo-beneficio:  $\text{Costo-beneficio} = (\text{Puntaje técnico} / \text{Costo de licenciamiento}) \times 100$  (Según la "Guía Técnica sobre evaluación de software en la administración pública")

## 8. CONCLUSIONES:

De acuerdo a la evaluación realizada en el presente documento, se recomienda la adquisición de software Antispam, que contenga las herramientas necesarias para la protección de los correos electrónicos institucionales, que coadyuve a la protección de la información crítica de la ANA; además de garantizar la confidencialidad, integridad y disponibilidad de la información.

En tal sentido, de acuerdo al presente documento donde se determinaron los atributos y/o características mínimas que deben ser considerados para la evaluación del software Antispam que cubra las necesidades de la Autoridad Nacional del Agua, donde se demuestra que la mejor alternativa para la institución es **SOPHOS**, ya que, a pesar de tener un puntaje técnico ligeramente inferior a Cisco, presenta un mejor costo beneficio, por lo que se recomienda su adquisición. Sin embargo, esto no excluye a participar del proceso de selección al software Cisco.



PERÚ

Ministerio  
de Desarrollo Agrario  
y Riego

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”  
“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración  
de las heroicas batallas de Junín y Ayacucho”

## 9. ANEXOS:

- Anexo 1: Sophos - Central Email Advanced
- Anexo 2: Cisco - Secure Email Cloud Gateway

## 10. FIRMAS:

Atentamente,

## FIRMADO DIGITALMENTE

**ALBERTO ADRIAN LOZA ROMERO**

PROFESIONAL

DIRECCIÓN DEL SISTEMA NACIONAL DE INFORMACIÓN DE RECURSOS HÍDRICOS

**ISMAEL EDWIN SALAZAR VILLAVICENCIO**

DIRECTOR

DIRECCIÓN DEL SISTEMA NACIONAL DE INFORMACIÓN DE RECURSOS  
HÍDRICOS

