



PERÚ

Presidencia del Consejo de Ministros

Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre OSINFOR

"Decenio de la igualdad de oportunidades para mujeres y hombres"
"Año de la lucha contra la corrupción y la impunidad"

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE N° 007-2019-OSINFOR/05.1

LICENCIAS DE SOFTWARE ANTISPAM

1. NOMBRE DEL ÁREA

Oficina de Tecnología de la Información

2. RESPONSABLES DE LA EVALUACIÓN

Ing. Gustavo Artica Cuyubamba - Jefe de la Oficina de Tecnología de la Información
Juan Praelli Bueno – Especialista en administración de redes

3. FECHA

1 de julio del 2019

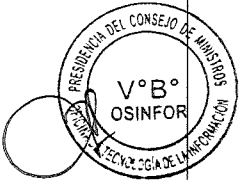
4. JUSTIFICACIÓN

El Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre ha contado en el último periodo anual con la solución de gateway antispam SpamTitan. Esta solución ha trabajado de manera adecuada en la protección de las estaciones de trabajo, servidores y sistemas informáticos de la Institución. Sin embargo, el período anual contratado para la actualización de parches y firmas de virus ha finalizado, por lo cual los equipos de la institución se encontrarán expuestos ante nuevas amenazas de spam y correos maliciosos que no se encuentren registrados en las bases de datos de la aplicación de seguridad.

Por tal motivo, con el objetivo de garantizar la protección de los equipos y la información de la institución, así como la continuidad de los servicios que permiten el cumplimiento de las labores de los usuarios, se requiere la adquisición de nuevas licencias para el siguiente periodo anual. Debido al aumento de personal y computadoras por los diversos proyectos que lleva a cabo la entidad, para el nuevo periodo anual se debe considerar la adquisición del licenciamiento para al menos 500 buzones de correo electrónico.

La solución de software antispam deberá proteger a todos los buzones de correo electrónico institucional y cumplir con las siguientes especificaciones mínimas:

Table with 4 columns: Características y condiciones, Software, Licencias, Vigencia mínima. Includes a table for software specifications and a section for characteristics.



Handwritten signature

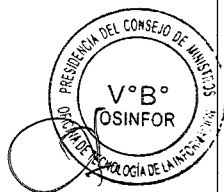
- Debe contar con un motor de escaneo de virus sobre SMTP.
- La consola de administración podrá ser accedida por medio de una interfaz web.
- Debe permitir la creación de cuentas basadas en roles para administración remota.
- Debe contar con las siguientes funcionalidades al nivel de protocolo SMTP:
  - Comprobación de DNS Lookup.
  - Detección de spam, virus, phishing y spyware
  - Filtro Anti-spoofing
  - Detección heurística
  - Filtro basado en palabras claves, tamaño y contenido.
  - Soporte nativo para el uso de SPF (Sender Policy Framework)
  - Lectura y validación de firmas DKIM
- Debe integrarse con servicios de directorio Microsoft Active Directory, y OpenLDAP.
- Debe permitir integrarse con "Real Time Blackhole List" (RBLs)
- Debe ser capaz de bloquear por dominios y direcciones IP, definiendo quién no puede ingresar (listas negras personalizadas)
- Debe permitir registrar a servidores que hacen relay.
- Debe permitir pasar correos sin que sean filtrados por las reglas existentes configuradas en el mismo software.
- Debe poder redireccionar el mensaje a una cuenta o grupo de cuentas de correo que se designe, además de permitir enviar a cuarentena los tipos de mensajes que se designe.
- Debe poder enviar notificaciones al remitente, destinatario, administrador y a una cuenta o grupo de cuentas que se designe cuando el mensaje cumpla con una regla específica.
- Debe poder definir reglas para correo entrante y saliente y ser aplicadas en forma independiente llegando a un nivel de clasificación de usuario y por categorías.
- Debe permitir bloquear correos por tipo de archivo adjunto tales como de video, sonido, ejecutables y gráficos (formato real del archivo, no por extensión).
- La consola debe permitir visualizar los registros de seguimiento de correos, eventos del sistema, eventos de políticas, eventos de MTA, desempeño del servidor; la revisión o búsqueda de correos recibidos, enviados, filtrados, en cuarentena o rechazados; así como tomar acciones sobre los correos retenidos en cuarentena, como por ejemplo eliminarlos o liberarlos.
- Debe proveer herramientas que permitan respaldar y restaurar completamente la configuración del servidor o appliance antispam.

#### **GARANTÍA Y SOPORTE TÉCNICO**

- La garantía y soporte técnico debe ser 24x7x365, on-site, vía telefónica y/o correo electrónico, con tiempo de respuesta inmediato por vía telefónica, durante todo el periodo de vigencia de la solución.
- Se deberá actualizar el software con las nuevas versiones y parches que aparezcan durante el periodo de licencia; se deberá coordinar con la Oficina de Tecnología de la Información los mecanismos para la aplicación de dichas versiones, previo análisis de impacto.

#### **CAPACITACIÓN**

- Se deberá incluir un curso de capacitación en la solución, al menos para diez (10) personas, con un mínimo de cuatro (04) horas de



	<p>duración. El local y fecha para la capacitación deberán ser coordinados con la Oficina de Tecnología de la Información y aprobados por esta. Se debe brindar constancia de participación para cada uno de los asistentes. Los certificados de capacitación deberán ser entregados dentro de los 30 días calendarios siguientes de realizado el curso.</p>
--	--

## 5. ALTERNATIVAS

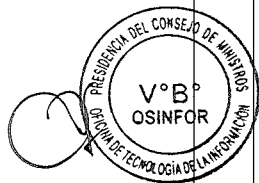
Se han elegido las siguientes alternativas de software antispam para su evaluación, en razón a la experiencia sobre su desempeño, así como su presentación anterior ante la entidad en estudios de mercado y procesos de selección, lo cual garantiza la existencia de varios proveedores que distribuyan y brinden soporte a estas marcas en Perú.

- TitanHQ SpamTitan Gateway
- Sophos Email Appliance

## 6. ANÁLISIS COMPARATIVO TÉCNICO

### 6.1. Descripción de métricas

Nº	Atributo	Descripción	Escala
<b>ATRIBUTOS INTERNOS</b>			
1	Seguridad y defensa contra spam y malware	Comprobación de DNS Lookup. Detección de spam, virus, phishing y spyware Filtro Anti-spoofing Detección heurística Filtro basado en palabras clave, tamaño y contenido	15
2	Listas personalizadas	Debe permitir integrarse con "Real Time Blackhole List" (RBLs) Debe ser capaz de bloquear por dominios y direcciones IP, definiendo quién no puede ingresar (listas negras personalizadas) Debe permitir registrar a servidores que hacen relay.	10
3	Reglas para correos entrantes y salientes	Debe permitir pasar correos sin que sean filtrados por las reglas existentes configuradas en el mismo software. Debe poder redireccionar el mensaje a una cuenta o grupo de cuentas de correo que se designe, además de permitir enviar a cuarentena los tipos de mensajes que se designe. Debe poder enviar notificaciones al remitente, destinatario, administrador y a una cuenta o grupo de cuentas que se designe cuando el mensaje cumpla con una regla específica. Debe poder definir reglas para correo entrante y saliente y ser aplicadas en forma independiente llegando a un nivel de clasificación de usuario y por categorías.	10
4	Bloqueo por tipo de archivos	Debe permitir bloquear correos por tipo de archivo adjunto tales como de video, sonido, ejecutables y gráficos (formato real del archivo, no por extensión).	5
<b>ATRIBUTOS EXTERNOS</b>			
5	Actualizaciones	Actualizaciones automáticas y programadas de las bases de datos y desde una consola de administración.	15
6	Administración	Administración, instalación, actualización y	15



B

		monitoreo desde una consola de administración central web. Debe permitir visualizar los registros de seguimiento de correos, eventos del sistema, eventos de políticas, eventos de MTA, desempeño del servidor; la revisión o búsqueda de correos recibidos, enviados, filtrados, en cuarentena o rechazados; así como tomar acciones sobre los correos retenidos en cuarentena, como por ejemplo eliminarlos o liberarlos.	
	<b>ATRIBUTOS DE USO</b>		
7	Alertas y reportes	El software deberá generar reportes configurables, automáticos y gráficos.	10
8	Documentación	El software debe tener manuales detallados de instalación y de configuración.	10
9	Productividad	El software debe tener el menor impacto sobre los recursos del sistema, de modo que se asegure una velocidad normal de procesamiento en los equipos.	10
		<b>TOTAL</b>	<b>100</b>

## 6.2. Puntajes

Nº	Atributo	TitanHQ SpamTitan Gateway	Sophos Email Appliance
	<b>ATRIBUTOS INTERNOS</b>		
1	Seguridad y defensa contra spam y malware	14	14
2	Listas personalizadas	9	10
3	Reglas para correos entrantes y salientes	10	10
4	Bloqueo por tipo de archivos	5	5
	<b>ATRIBUTOS EXTERNOS</b>		
5	Actualizaciones	15	15
6	Administración	15	15
	<b>ATRIBUTOS DE USO</b>		
7	Alertas y reportes	10	10
8	Documentación	9	9
9	Productividad	10	10
	<b>TOTAL</b>	<b>97</b>	<b>98</b>

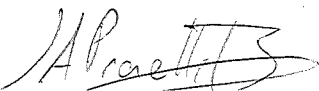
## ANÁLISIS COMPARATIVO DE COSTO-BENEFICIO

- Productos: TitanHQ SpamTitan Gateway. Costo estimado: **S/. 41280,00** (costo estimado sobre la base del precio de referencia para 250 usuarios en el portal web del fabricante, y considerando un multiplicador de 4 para el tipo de cambio y la importación)
- Productos: Sophos Email Appliance. Costo estimado: **S/ 33000,00** (sobre la base de la oferta de SECURITY LABS PERÚ S.A.C.,)

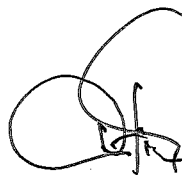

## 8. CONCLUSIONES

- Se determina que ambos productos evaluados son adecuados para la protección de la seguridad de la información institucional. Dado que las prestaciones son similares, lo más recomendable es renovar la solución actual para reducir labores de migración y cambios, siempre y cuando las condiciones económicas sean favorables para la entidad.

9. FIRMAS



**Juan Praelli Bueno**  
Especialista en Administración de Redes  
Oficina de Tecnología de la Información

**Ing. Gustavo Artica Cayubamba**  
Jefe  
Oficina de Tecnología de la Información

[https://www.titanhq.com/pricing/product\\_type=spamtitan](https://www.titanhq.com/pricing/product_type=spamtitan)

Simple and transparent pricing

TitanHQ  
**SpamTitan**

250 Users

Monthly

1.08 \$ Per user Monthly

Discount -

Savings -

268.75 \$ Total Price

BUY NOW

TitanHQ  
**SpamTitan**

250 Users

1 Year

0.97 \$ Per user Monthly

Discount 10.00%

Savings \$ 322.5

2902.5 \$ Total Price

BUY NOW

TitanHQ  
**SpamTitan**

250 Users

2 Year

0.86 \$ Per user Monthly

Discount 20.00%

Savings \$ 1290

5160 \$ Total Price

BUY NOW

TitanHQ  
**SpamTitan**

250 Users

3 Year

0.75 \$ PER USER MONTHLY

Discount 30.00%

Savings \$ 2902.5

6772.5 \$ Total Price

BUY NOW




## COTIZACIÓN DE PRODUCTOS:

Nombre de cliente: Organismo de Supervisión de los Recursos Forestales (OSINFOR)  
R.U.C.: 20522224783  
Contacto: Juan Praelli  
Teléfono: 6157373  
email: [jpraelli@osinfor.gob.pe](mailto:jpraelli@osinfor.gob.pe)

PRODUCTO	CANTIDAD	TOTAL INCLUIDO ICV
SOPHOS EMAIL PROTECTION	500 licencias	S/. 33,000.00

### INFORMACION DE FACTURACION:

- PAGO: Previa conformidad
- PLAZO DE ENTREGA: – Hardware Appliance 45 días y Virtualizado en plazo de 6 días.
- La previsión de entrega informada en esta propuesta es un estimado, estando sujeta a confirmación de disponibilidad en el momento de la aceptación. Atrasos en la fabricación/entrega/disponibilidad del material por el fabricante y otros eventos podrán afectar la previsión final de entrega.
- GARANTÍA: La garantía es de responsabilidad del fabricante. El plazo es estipulado de acuerdo con la política definida por el fabricante, para cada uno de sus productos.

