"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año de la unidad, la paz y el desarrollo"

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE Nº 00007-2023-OSINFOR/05.1

LICENCIAS DE SOFTWARE ANTISPAM

1. NOMBRE DEL ÁREA

Oficina de Tecnologías de la Información

2. RESPONSABLES DE LA EVALUACIÓN

Ing. Gustavo Artica Cuyubamba - Director de la Oficina de Tecnologías de la Información
Juan Praelli Bueno – Especialista en Administración de Redes

3. FECHA

28 de setiembre del 2023

4. JUSTIFICACIÓN

El Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre ha contado en los últimos años con soluciones de gateway antispam Trend Micro y TitanHQ. 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 contratado para la actualización de la solución está por finalizar, 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 de dos años. 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>
<tr>
<td>Características y condiciones</td>
<td>
A. PRESTACION PRINCIPAL
<table>
<tr><th>Software</th><th>Licencias</th><th>Vigencia mínima</th></tr>
<tr><td>ANTISPAM</td><td>Licencia corporativa para 500 buzones de correo electrónico</td><td>2 años</td></tr>
</table>
Características

La solución de antispam deberá proteger al servicio de correo electrónico institucional (soporte para servidores Exchange 2013, 2016 y 2019) y cumplir con las siguientes especificaciones mínimas:

• Debe ser una solución de gateway en software (appliance virtual, certificado para trabajar sobre VMware) o que combine software
</td>
</tr>
</table>

	y hardware. Debe poder instalarse en un ambiente de virtualización VMware. La entidad proporcionará los recursos físicos de hardware en su plataforma de virtualización (vSphere 8) en el caso de que la solución propuesta sea en software o appliance virtual. Si la solución propuesta incluye hardware, es responsabilidad del contratista brindar todos los componentes que sean necesarios para su funcionamiento. • 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: o Comprobación de DNS Lookup. o Detección de spam, virus, phishing y spyware o Filtro Anti-spoofing o Detección heurística o Filtro basado en palabras claves, tamaño y contenido. o Soporte nativo para el uso de SPF (Sender Policy Framework) o Lectura y validación de firmas DKIM • Debe integrarse con servicios de directorio Microsoft Active Directory, y OpenLDAP. • Debe integrarse con RBLs públicas o propias del fabricante. • 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 especifica. • 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. **<u>Capacitación</u>** • Se deberá brindar dentro del plazo de ejecución de la prestación principal un curso/taller de capacitación virtual y/o presencial sobre las soluciones de antivirus, antispam y control de contenido

	web que se implementarán para un mínimo de **diez (10) personas**, con una duración mínima de **nueve (09) horas**. Los locales y fechas para la capacitación deberán ser coordinados con la Oficina de Tecnologías de la Información. El CONTRATISTA brindará constancia o certificado de participación para cada uno de los asistentes. Los certificados de capacitación deberán ser entregados dentro del único entregable correspondiente a la prestación principal que se indica en el numeral 5.3 de las especificaciones técnicas. **Condiciones generales** • Los postores deberán adjuntar documentación técnica de las soluciones ofertadas, tales como folletos, catálogos, fichas técnicas o similares, hojas técnicas, hojas de datos, brochures, manuales y/o cartas de los fabricantes donde se mencione el cumplimiento técnico de las características requeridas, en español o en idioma original, para acreditar o verificar el cumplimiento de los requerimientos técnicos mínimos. • Se deberá acreditar para la presentación de la oferta que el postor es representante autorizado en el Perú, para brindar la comercialización de las soluciones ofertadas; para lo cual se debe acreditar mediante el siguiente documento: Carta del fabricante, que acredite que el postor es representante y/o distribuidor y/o partner y/o revendedor autorizado en el Perú, para la venta y soporte de las soluciones ofertadas (antispam, antivirus y control de contenido web). La Entidad se reserva el derecho de verificar lo propuesto por el postor, verificando su condición de representante y/o distribuidor y/o partner y/o revendedor autorizado por el fabricante. En el caso de consorcios, cada integrante del consorcio que se hubiera comprometido a ejecutar las obligaciones vinculadas directamente al objeto de la convocatoria debe acreditar este requisito. • El contratista no deberá interferir con las actividades de OSINFOR, por lo cual la ejecución de las tareas se podrá programar fuera del horario laboral de ser necesario, en coordinación con la Oficina de Tecnologías de la Información y con la autorización de la administración del Edificio Primera Visión en el caso de trabajos presenciales. Se brindarán las facilidades y espacios de trabajo durante horario de oficina siempre y cuando las labores por realizar no interrumpan las operaciones del OSINFOR. Los trabajos de instalación y configuración que no requieran la visita a la entidad se pueden realizar de manera remota, en coordinación con la Oficina de Tecnologías de la Información del OSINFOR. • Para la realización de cualquier trabajo de implementación que deba ser efectuado dentro de las instalaciones de la entidad, OSINFOR garantizará al contratista todos los accesos necesarios teniendo a su cargo la responsabilidad de gestionar las autorizaciones de ingreso necesarias y desocupar los espacios, oficinas y/o pasillos donde vayan a ser ejecutados los respectivos trabajos de instalación.

	▪ La instalación y configuración de las soluciones ofertadas deberá ser realizada y supervisada por lo menos por un especialista (PERSONAL CLAVE) que cumpla con los siguientes requisitos, los cuales serán acreditados por el postor en la presentación de su oferta: - Bachiller universitario o técnico titulado en Ingeniería de Redes, y/o Telecomunicaciones, y/o Eléctrica, y/o Electrónica, y/o Informática, y/o Sistemas, y/o Computación, y/o Industrial, y/o Computación y Sistemas, y/o Redes y Comunicaciones de Datos, con experiencia acreditada no menor de 02 (dos) años, en entidades públicas y/o privadas, en la ejecución de proyectos de implementación y/o configuración de sistemas, soluciones y/o software de seguridad informática, seguridad de la información y/o ciberseguridad, o similares. - Deberá contar con certificaciones vigentes y/o cursos de especialización y/o capacitación en sistemas y/o soluciones y/o software de seguridad informática, seguridad de la información y/o ciberseguridad, o similares. ▪ Las soluciones ofertadas no pueden estar catalogadas como "fuera de venta" (END-OF-LIFE) por el fabricante. • Una vez culminada la instalación, configuración y capacitación se suscribirá el acta de inicio de la prestación accesoria, firmada por los representantes del CONTRATISTA y la Oficina de Tecnologías de la Información del OSINFOR. En dicha acta se consignará la fecha en la que inicia el plazo de 2 años para la vigencia de las soluciones y la prestación de la garantía y soporte técnica. **B. <u>PRESTACION ACCESORIA: GARANTÍA Y SOPORTE TÉCNICO</u>** • La garantía comercial para todas las soluciones deberá ser por un periodo de 2 años contabilizado desde la fecha indicada en el acta de inicio de prestación accesoria. Proporciona la actualización de las licencias del producto a la última versión disponible, incluyendo su instalación, configuración y despliegue; así como el soporte técnico y la corrección de errores y/o incidencias de fallas, averías o mal funcionamiento de las soluciones. La atención debe ser 24x7x365, on-site, vía telefónica y/o correo electrónico, durante todo el periodo de vigencia de las soluciones. El contratista puede brindar también acceso a un sistema de mesa de ayuda o mesa de servicio para el reporte de incidencias o requerimientos. • Se deberá actualizar el software con las nuevas versiones y parches que aparezcan durante el periodo de licencia, para lo cual se deberá coordinar con la Oficina de Tecnologías de la Información los mecanismos para la programación y aplicación de dichas versiones, previo análisis de impacto. • El contratista, al momento del inicio de ejecución del contrato, debe entregar a la Oficina de Tecnologías de la Información el procedimiento de escalamiento ante averías. El contratista debe contar con un procedimiento para el reporte de averías, el cual

debe contemplar, entre otras cosas, la asignación de un número, código o ticket de atención que facilite el seguimiento de la falla reportada. Deberá informar al inicio de servicio las direcciones de correo electrónico y los números telefónicos para el reporte de averías, así como el (los) nombre(s) de las áreas y/o personal técnico de contacto de cada nivel de escalamiento.

- Para atención de requerimientos e incidencias, el/la contratista deberá tener en cuenta lo siguiente:

  - Se entenderá por requerimiento a las configuraciones adicionales solicitadas por el OSINFOR, en las cuales se busque personalizar y/o mejorar y/o actualizar y/o incrementar y/o perfeccionar la administración y/o funcionamiento de las soluciones en beneficio de los usuarios y la postura de seguridad del OSINFOR; para tal efecto el/la contratista podrá hacer uso de las horas de soporte técnico proactivo contratadas.

  - Se entenderá por incidencia a la ocurrencia de errores, fallas, averías o mal funcionamiento de las soluciones, así como la irrupción de una amenaza que afecta la seguridad de los activos de información del OSINFOR. La atención y solución de incidencias no consumirá las horas de soporte técnico proactivo.

- El contratista deberá atender las incidencias que ocurran durante el plazo de la prestación accesoria, de manera ilimitada, para todos los componentes de las soluciones, en formato 24x7x365 (24 horas durante los 7 días de la semana).

- El contratista brindará 80 horas de soporte técnico proactivo (20 horas por cada semestre) para la atención de requerimientos, de corresponder.

- El contratista debe generar el número, código o ticket de atención una vez que se reporte la incidencia o avería mediante llamada telefónica, correo electrónico o sistema de mesa de ayuda. Si el reporte es vía telefónica, el operador brindará el número, código o ticket de atención para el seguimiento de la incidencia reportada. Si el reporte es vía correo electrónico o web, el sistema de mesa de ayuda del contratista deberá automáticamente generar un número de ticket para su seguimiento. El número, código o ticket de atención deberá ser asignado o generado en un tiempo máximo de 30 minutos desde el reporte realizado por el OSINFOR

- El tiempo de respuesta para la atención de incidentes y/o requerimientos será de acuerdo al siguiente detalle:

Tiempos	Incidencias	Requerimientos
Tiempo de atención	30 minutos (en 24x7)	4 horas (L-V, entre las 8:00 y 18:00 horas)
Tiempo de solución	4 horas (en 24x7)	4 días útiles (L-V, entre las 8:00 y 18:00 horas)

	- Tiempo de atención: Es el tiempo máximo en el cual el contratista debe iniciar la atención de la avería/incidencia o requerimiento/consulta; se cuenta desde la generación/asignación del número, código o ticket de atención y finaliza cuando el contratista inicia la atención. - Tiempo de solución: Periodo de tiempo transcurrido desde que el contratista se pone en contacto con el OSINFOR (de manera presencial o remota) para iniciar la atención, y finaliza cuando se completa el requerimiento o hasta solucionar la incidencia o encontrar una solución alternativa (*workaround*) a la misma. El tiempo máximo se indica en el cuadro anterior, contado a partir de la generación/asignación del número, código o ticket de atención.

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.

- Kaspersky Security Mail Gateway
- TitanHQ SpamTitan Gateway

6. ANÁLISIS COMPARATIVO TÉCNICO

6.1. Descripción de métricas

Nº	Atributo	Descripción	Escala
	ATRIBUTOS INTERNOS		
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 especifica.	10

		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.	
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
	ATRIBUTOS EXTERNOS		
5	Actualizaciones	Actualizaciones automáticas y programadas de las bases de datos y desde una consola de administración.	15
6	Administración	Administración, instalación, actualización y 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.	15
	ATRIBUTOS DE USO		
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
		TOTAL	**100**

6.2. Puntajes

Nº	**Atributo**	**Kaspersky Security Mail Gateway**	**TitanHQ SpamTitan Gateway**
	ATRIBUTOS INTERNOS		
1	Seguridad y defensa contra spam y malware	14	14
2	Listas personalizadas	9	9
3	Reglas para correos entrantes y salientes	10	10
4	Bloqueo por tipo de archivos	5	5
	ATRIBUTOS EXTERNOS		
5	Actualizaciones	15	15
6	Administración	15	15
	ATRIBUTOS DE USO		
7	Alertas y reportes	10	10
8	Documentación	9	8
9	Productividad	10	10
	TOTAL	**97**	**96**

7. ANÁLISIS COMPARATIVO DE COSTO-BENEFICIO

- Producto: Kaspersky Secure Mail Gateway. Costo estimado: **S/ 17,936.00** (sobre la base de la cotización de BAFING S.A.C., tipo de cambio S/ 3.80: 4000x1.18x3.8)

- Productos: TitanHQ SpamTitan Gateway. Costo estimado: **S/ 12,000.00** (sobre la base de la cotización de INNOVA TECNOLOGIA CORP 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

Firmado digitalmente por
Ing. Gustavo Artica Cuyubamba
Director
Oficina de Tecnologías de la Información

Firmado digitalmente por
Juan Praelli Bueno
Especialista en Administración de Redes
Oficina de Tecnologías de la Información

OSINFOR
Firmado digitalmente por: ARTICA CUYUBAMBA Gustavo FAU 20522224783 soft
Motivo: En señal de conformidad
Fecha: 28/09/2023 17:35:30-0500

OSINFOR
Firmado digitalmente por: PRAELLI BUENO Juan Antonio FAU 20522224783 soft
Motivo: Soy el autor del documento
Fecha: 28/09/2023 16:44:45-0500

BAFING

PROPUESTA ECONÓMICA

EDR, ANTISPAM Y FILTRO WEB				
Ítem	**Descripción**	**Precio Unit.**	**Cant**	**Precio Total**
1	**Kaspersky Total Security for Business** ✓ Incluye 2 años de Kaspersky Software Business Support	**$ 16.00**	**500**	**$8,000.00**
2	**Kaspersky Secure Mail Gateway** ✓ Incluye 2 años de Kaspersky Software Business Support	**$4,000.00**	**1**	**$4,000.00**
3	**Licencia FortiProxy – VMO2** ✓ Virtual appliance designed for all supported platforms. 4x vCPU core, Unlimited RAM and 2TB Disk (2 year) Funciones: ✓ SWG Protection ✓ Web & Video Filtering ✓ DNS Filtering ✓ Application Control ✓ DLP ✓ IPS ✓ AV ✓ V, Botnet (IP/Domain) ✓ Sandbox Cloud including Virus Outbreak and Content Disarm & Reconstruct	**$6,664.00**	**1**	**$6,664.00**
4	**Forticare Premium Support** ✓ FortiProxy-VM02 1 Year FortiCare Premium Support	**$1,576.00**	**2**	**$1,576.00**
5	**Valor Agregado** ✓ 03 Horas de capacitación (online) de uso y manejo de la plataforma Kaspersky Total Security for Business (4 personas) ✓ 03 Horas de capacitación (online) de uso y manejo de la plataforma FortiProxy (4 personas)	**$ 0.00**	**$ 0.00**	**$ 0.00**

+51 1 225 9900
info@bafing.com
www.bafing.com
@BafingSAC
Av. Del Parque Sur 560, San Borja, Lima, Perú

Ciberseguridad
Smart Buildings
eHealth

PROPUESTA ECONOMICA
ORGANISMO DE SUPERVISIÓN DE LOS RECURSOS FORESTALES Y DE FAUNA SILVESTRE – OSINFOR

ÍTEM	DESCRIPCIÓN DEL BIEN Y/O SERVICIO	SUSCR	CANT	P.U.	COSTOS
01	**PRESTACIÓN PRINCIPAL** Adquisición de licencias Antivirus, Antispam y Filtro Web G Data Endpoint Protection Business	2 años	500	S./30,000.00	S./30,000.00
02	**PRESTACIÓN PRINCIPAL** Adquisición de licencias Antivirus, Antispam y Filtro Web SpamTitan HQ Gateway	2 años	500	S./12,000.00	S./12,000.00
03	**PRESTACIÓN PRINCIPAL** Adquisición de licencias Antivirus, Antispam y Filtro Web WebTitan HQ Gateway	2 años	500	S./23,000.00	S./23,000.00
04	**PRESTACIÓN ACCESORIA** Servicios Garantía de Soporte - Despliegue e implementación al 100% - Informes de performance semestrales - Soporte técnico a incidencias ilimitado - Cobertura de soporte 24x7x365 **Capacitación** - Capacitación con certificación oficial - Asesoría en configuraciones y reglas	2 años	NA	S./5,500.00	S./5,500.00
				SUBTOTAL	S./70,500.00
				IGV	S./12,690.00
				TOTAL	S./83,190.00

OBSERVACIONES COMERCIALES

- Moneda : Soles
- Impuestos : Incluye IGV
- Vigencia de la oferta : 60 dias
- Entrega de licencias : 48 horas
- Implementación : 05 dias
- Garantía : 02 años
- Forma de pago : Previa conformidad

DATOS DEL PROVEEDOR

- Razón Social : INNOVA TECNOLOGIA CORP S.A.C.
- RUC : 20601100593
- Dirección : Av. Los Constructores 1125, urb. santa patricia, La Molina
- Contacto : Jimmy Jauregui
- E-mail : administracion@innovatc.com
- Teléfonos : +51 348 0842 | # +51 987 303 162

INNOVA TC S.A.C.
ventas@innovatc.com | soporte@innovatc.com
+ 511 348-0842
Av. Los Constructores 1125, Urb. Santa Patricia La Molina
https://innovatc.com/