"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 Nº 006-2019-OSINFOR/05.1

LICENCIAS DE SOFTWARE ANTIVIRUS

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 antivirus ESET Endpoint Security. 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 virus y malware 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, así como por la necesidad de proteger los equipos móviles como tablets y smartphones de acuerdo a las normas del Sistema de Gestión de la Seguridad de la Información del OSINFOR, para el nuevo periodo anual se debe considerar la adquisición del licenciamiento para al menos 500 equipos.

PRESIDENCIA DEL CONSEJO DE MINISTROS V°B° OSINFOR OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN

La solución de software antivirus deberá proteger a todos los equipos informáticos (estaciones de escritorio, móviles y servidores) y cumplir con las siguientes especificaciones mínimas:

Características y condiciones	Software	Licencias	Vigencia mínima
	ANTIVIRUS	1 Licencia Corporativa para **500** equipos (estaciones de trabajo, móviles, servidores)	2 años
	CARACTERISTICAS La solución de antivirus deberá proteger a todos los equipos informáticos (estaciones de escritorio, móviles y servidores) y cumplir con las siguientes especificaciones mínimas:		

	a) Solución antimalware • La solución debe brindar protección por lo menos para los siguientes sistemas operativos de escritorio: Windows 7/8/10; y para los siguientes sistemas operativos de servidor: Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019. • La solución debe brindar protección y gestionar dispositivos móviles con sistemas operativos Windows, Android y iOS, con funciones para protección de datos y cifrado de la información. • La solución de protección para estaciones finales deberá estar basada no solo en detección de firmas, sino también en comportamiento, heurística y reputación de archivos y web, basada en una nube privada dedicada a proteger proactivamente de malware, sea conocido en la base de firmas o sin estar contenido en ellas. • Deberá poderse configurar con al menos dos tipos de perfiles: uno cuando el usuario se conecte dentro de la red corporativa; y el segundo, cuando se conecte fuera. • Detectar, analizar y eliminar programas maliciosos, como virus, spyware, gusanos, troyanos, keyloggers, adware, rootkits, phishing, bots, ransomware. entre otros, de forma automática y en tiempo real. Detectar y proteger al equipo contra acciones maliciosas que se ejecutan en navegadores Web. • Para el escaneo de archivos, la solución deberá al menos permitir configurar: o Escaneo de cualquier tipo de archivo o Escaneo basado en el identificado de tipo de archivo o Escaneo de archivos basado en extensiones específicas o Escaneo basado en extensiones de archivos recomendados por el fabricante o Escaneo basado en extensiones de archivos definidas por el administrador o Escaneo de archivos comprimidos • Manejo de niveles de seguridad para evitar la navegación Web a sitios maliciosos cuando los usuarios se encuentran dentro o fuera de la red corporativa. Permitir reclasificar sitios web. Permitir editar la lista de URL para dar acceso a sitios que se encuentren bloqueados a nivel general, grupos o personal. El sistema de protección web no deberá depender de ningún navegador específico. • Evitar o monitorear que un programa con comportamiento sospechoso pueda duplicar o inyectar archivos de sistema similares, modificar el archivo de HOST, incrustar plugins en los navegadores de Internet, instalar librerías de programas maliciosos, instalar nuevos servicios, modificar archivos de sistema o instalar servicios o programas que se inicien al arrancar la estación de trabajo. • Controlar el acceso a dispositivos de almacenamiento USB, CD/DVD y carpetas compartidas. La solución debe poder crear una lista blanca de dispositivos USB autorizados para su uso en la institución. Para los dispositivos USB, CD/DVD y carpetas compartidas, el antimalware deberá permitir configurar que el usuario tenga permisos de control total, modificación, solo lectura, solo lectura y ejecución, o evitar que el usuario pueda tener acceso al contenido del dispositivo. La solución deberá evitar infecciones provocadas por la ejecución del archivo autorun.inf en un dispositivo USB al momento de ser conectado. • La solución deberá poseer módulos de firewall e IDS/IPS, cuyo

PRESIDENCIA DEL CONSEJO DE MINISTROS
V°B°
OSINFOR
OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN

	manejo debe estar integrado en la consola de administración de la solución. Monitoreo de tráfico de red de entrada y salida, de desviaciones de protocolo o contenido que podrían indicar un ataque. Permitir el bloqueo de puertos específicos y accesos indebidos que no estén en la tabla de políticas definidas por el administrador. Capaz de crear reglas de bloqueo/acceso para protocolos y aplicaciones. Protección proactiva contra ataques de "buffer overflow". Capacidad de detectar y bloquear paquetes "exploit" que atacan vulnerabilidades de sistemas operativos Windows, aplicaciones comunes y bases de datos. Creación de políticas basadas en distintos perfiles. Permitir configuración y manipulación de políticas de firewall a través de prioridades. Permitir la creación de reglas de firewall por protocolos, dirección IP, dirección MAC y/o puerto de origen; y dirección IP, dirección MAC y/o puerto destino. • Brindar protección al usuario final contra exploits de vulnerabilidades, contra ataques de denegación de servicios, contra tráfico de red ilegitimo, contra amenazas web, contra ataques de día cero, contra amenazas avanzadas bloqueando vulnerabilidades conocidas y desconocidas, sin impactar en el rendimiento de la red. **b) Consola centralizada de administración** • La solución deberá contar con una herramienta que consolide la administración de todas las consolas antivirus que se instalen. La consola de administración central deberá poder desplegar el licenciamiento a las demás consolas antivirus. Capacidad para administrar otras consolas de su mismo tipo, localizadas en segmentos diferentes de la red y proporcionar la información de dichas consolas de manera remota. • Se debe poder instalar por lo menos en plataformas Windows Server 2012, 2012 R2 y 2016. • Debe permitir visualizar, de forma rápida y sencilla, el estado de las estaciones de trabajo y servidores, así como el estado y estadísticas de las infecciones generadas y permitir también visualizar las estaciones de trabajo y servidores donde ocurrió la detección o infección. • Visualizar, de forma rápida y sencilla, un resumen del estado de las actualizaciones de firmas en las estaciones de trabajo y servidores, cantidad de equipos actualizados y desactualizados. • La consola de administración centralizada debe soportar actualizaciones desatendidas y remotas del mismo fabricante. Deberá tener la capacidad de conectarse automáticamente a Internet y bajar las actualizaciones necesarias para todos los productos antivirus. Capacidad para actualizarse de manera alternativa utilizando un recurso compartido o medio de almacenamiento externo en caso de no contar con una conexión a Internet y desplegar la actualización a los productos antivirus que controla. • La consola deberá poseer un log de eventos detallados y en el ámbito general de todos los productos y consolas antivirus instalados en la red. • La consola central de administración deberá permitir y programas reportes consolidados. • La consola debe permitir la creación de diversos usuarios para su administración y con diferentes niveles de acceso. La consola deberá permitir una estructura jerárquica la cual ofrezca determinación en el control de acceso, como permisos y roles sobre

PRESIDENCIA DEL CONSEJO DE MINISTROS
V°B°
OSINFOR
OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN

	la solución. • La consola de administración centralizada debe poseer la capacidad de actualizar las políticas de seguridad desde el fabricante en caso de una epidemia mundial de malware. • Distribución automática y/o programada de actualizaciones para los distintos productos de antivirus. • Aplicar configuración de políticas por servidor o estación de trabajo, por grupo o por usuario de manera independiente. Importar o exportar configuraciones de políticas de un grupo de estaciones de trabajo a otro. • Integración con Active Directory para la asignación de roles y permisos de acceso a las configuraciones y administración de la consola; para el despliegue y configuración del agente antivirus; y para la identificación de grupos y/o usuarios del mismo para la generación de políticas desde la consola de administración. • Permitir generar un análisis de equipos que cuenten o no con una protección antimalware, basado en dominios o grupos de Directorio Activo. • Programación de escaneos y distribución de actualizaciones a los clientes de manera automática y manual. Actualización de sistema de firmas para clientes sin conectividad al servidor. Actualización de grupos de usuarios por agentes de actualización o repositorios distribuidos. **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 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.

PRESIDENCIA DEL CONSEJO DE MINISTROS
V°B°
OSINFOR
OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN

5. ALTERNATIVAS

Se han elegido las siguientes alternativas de software antivirus 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.

- ESET Endpoint Protection
- F-Secure Business Suite

6. ANÁLISIS COMPARATIVO TÉCNICO

6.1. Descripción de métricas

Nº	Atributo	Descripción	Escala
	ATRIBUTOS INTERNOS		
1	Sistemas operativos de estaciones de trabajo	Microsoft Windows 7/8/10	5
2	Sistemas operativos de servidores	Microsoft Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019	5
3	Sistemas operativos de dispositivos móviles	Windows, Android, iOS	5
4	Seguridad y defensa contra malware	El software antivirus debe ser capaz de proteger contra virus, troyanos, gusanos, spyware, adware, spam, ataques de día cero y otros tipos de malware.	10
5	Escaneo	El software debe tener la capacidad de detectar amenazas en todo tipo de archivos (incluyendo comprimidos, ocultos y en ejecución). El escaneo puede ser en tiempo real o en segundo plano, y se debe poder programar en forma remota a través de la consola de administración.	10
6	Control de dispositivos	Control de accesos a medios removibles (USB, CD/DVD)	5
	ATRIBUTOS EXTERNOS		
7	Actualizaciones	Actualizaciones automáticas y programadas de las bases de datos y desde una consola de administración.	10
8	Instalación y despliegue	La instalación y despliegue del software y del agente de red en los equipos finales debe poder hacerse tanto desde la consola de administración como desde un medio externo (CD/DVD, USB)	5
9	Administración	Administración, instalación, actualización y monitoreo desde una consola de administración central. Debe permitir un control granular y flexible por equipos y grupos con la opción de que los subgrupos hereden o no políticas.	10
10	Licencias	La solución debe permitir el manejo flexible de las licencias, de manera que puedan ser reasignadas en caso de cambios de equipo.	5
	ATRIBUTOS DE USO		
11	Alertas y reportes	El software deberá generar reportes configurables, automáticos y gráficos.	10
12	Documentación	El software debe tener manuales detallados de instalación y de configuración.	10
13	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**

PRESIDENCIA DEL CONSEJO DE MINISTROS
V°B°
OSINFOR
OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN

6.2. Puntajes

Nº	Atributo	ESET Endpoint Protection	F-Secure Business Suite
	ATRIBUTOS INTERNOS		
1	Sistemas operativos de estaciones de trabajo	5	5
2	Sistemas operativos de servidores	5	5
3	Sistemas operativos de dispositivos móviles	4	2
4	Seguridad y defensa contra malware	9	9

5	Escaneo	10	10
6	Control de dispositivos	5	5
	ATRIBUTOS EXTERNOS		
7	Actualizaciones	10	10
8	Instalación y despliegue	5	5
9	Administración	10	10
10	Licencias	5	5
	ATRIBUTOS DE USO		
11	Alertas y reportes	10	10
12	Documentación	10	10
13	Productividad	10	9
	TOTAL	**98**	**95**

7. ANÁLISIS COMPARATIVO DE COSTO-BENEFICIO

- Producto: ESET Endpoint Protection Advanced. Costo estimado: **S/ 25800,00** (sobre la base de la cotización de SECURITY LABS PERÚ S.A.C.)

- Producto: F-Secure Business Suite. Costo estimado: **S/ 33440.00** (estimado sobre la base de los precios de referencia en www.viruslogic.com y considerando un multiplicador de 4 para el tipo de cambio y la importación – 16.72x500x4)

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 de agente antivirus, 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

PRESIDENCIA DEL CONSEJO DE MINISTROS
OSINFOR
OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN

Ing. Gustavo Artica Cuyubamba
Jefe
Oficina de Tecnología de la Información

Security Labs

1. PROPUESTA ECONÓMICA

COTIZACIÓN – RN-EP20190502

PRODUCTO	PERIODO	CANTIDAD	PRECIO	
			UNITARIO Soles S/	TOTAL Soles S/
ESET Endpoint Protection Advanced *Incluye:* *ESET Endpoint Security* *ESET File Security* *ESET Mobile Security*	2 años	500	51.60	S/. 25,800.00

* Se adjunta brochure de la solución ofertada.

PRECIO EN SOLES, INCLUYE IGV

Forma de pago	:	Contado previa conformidad
Plazo de entrega	:	07 días calendario
Garantía	:	Todo el periodo de licenciamiento
Validez de la oferta	:	30 días

Si está de acuerdo con la presente cotización, generar la orden de servicio a:

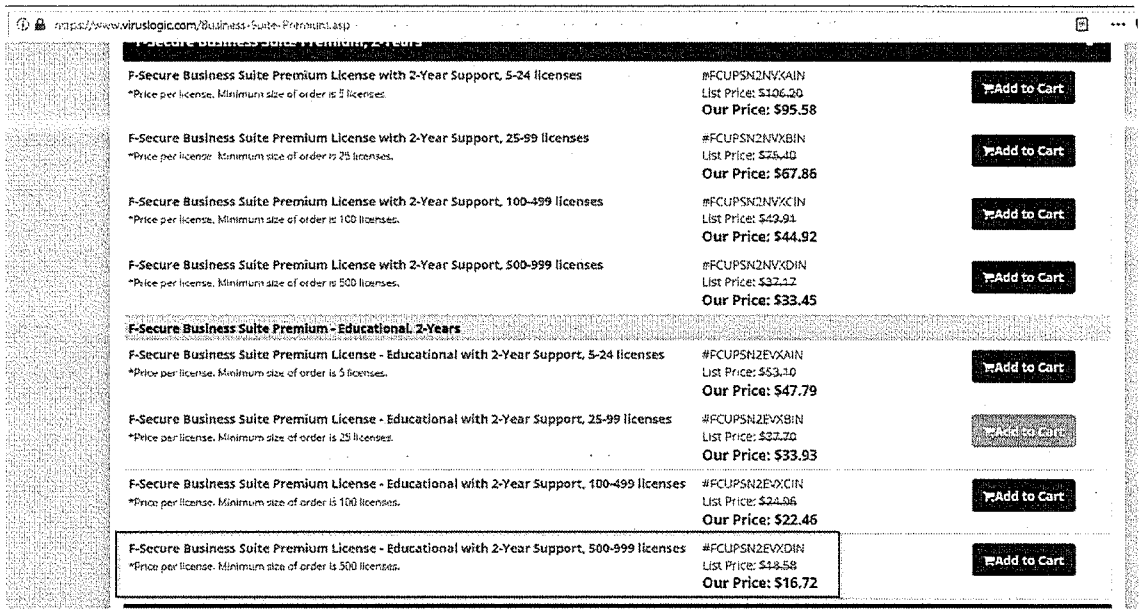
Razón Social	:	SECURITY LABS PERÚ S.A.C.
Ruc	:	20563462010
Dirección	:	Av. Guardia Civil 864 Of. 401, San Isidro - Lima
Correo electrónico:		ventas@securitylabs.pe
Teléfono:		(01)224-9898

2 de Mayo de 2019

Atentamente,

Enrique Palomino Ruidias
Consultor Corporativo

PRESIDENCIA DEL CONSEJO DE MINISTROS
V°B°
OSINFOR
OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN



F-Secure Business Suite Premium License with 2-Year Support, 5-24 licenses *Price per license. Minimum size of order is 5 licenses.	#FCUPSN2NVXAIN List Price: ~~$106.20~~ **Our Price: $95.58**	Add to Cart
F-Secure Business Suite Premium License with 2-Year Support, 25-99 licenses *Price per license. Minimum size of order is 25 licenses.	#FCUPSN2NVXBIN List Price: ~~$75.40~~ **Our Price: $67.86**	Add to Cart
F-Secure Business Suite Premium License with 2-Year Support, 100-499 licenses *Price per license. Minimum size of order is 100 licenses.	#FCUPSN2NVXCIN List Price: ~~$49.91~~ **Our Price: $44.92**	Add to Cart
F-Secure Business Suite Premium License with 2-Year Support, 500-999 licenses *Price per license. Minimum size of order is 500 licenses.	#FCUPSN2NVXDIN List Price: ~~$37.12~~ **Our Price: $33.45**	Add to Cart
F-Secure Business Suite Premium - Educational, 2-Years		
F-Secure Business Suite Premium License - Educational with 2-Year Support, 5-24 licenses *Price per license. Minimum size of order is 5 licenses.	#FCUPSN2EVXAIN List Price: ~~$53.10~~ **Our Price: $47.79**	Add to Cart
F-Secure Business Suite Premium License - Educational with 2-Year Support, 25-99 licenses *Price per license. Minimum size of order is 25 licenses.	#FCUPSN2EVXBIN List Price: ~~$37.70~~ **Our Price: $33.93**	Add to Cart
F-Secure Business Suite Premium License - Educational with 2-Year Support, 100-499 licenses *Price per license. Minimum size of order is 100 licenses.	#FCUPSN2EVXCIN List Price: ~~$24.96~~ **Our Price: $22.46**	Add to Cart
F-Secure Business Suite Premium License - Educational with 2-Year Support, 500-999 licenses *Price per license. Minimum size of order is 500 licenses.	#FCUPSN2EVXDIN List Price: ~~$18.58~~ **Our Price: $16.72**	Add to Cart

PRESIDENCIA DEL CONSEJO DE MINISTROS
OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN
V°B°
OSINFOR