"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 00006-2023-OSINFOR/05.1

LICENCIAS DE SOFTWARE ANTIVIRUS

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 la última década con soluciones de antivirus Trend Micro, Eset y G Data. Estas soluciones han 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 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 de dos años. Se debe considerar la adquisición del licenciamiento para al menos 500 equipos.

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:

<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>ANTIVIRUS</td><td>Licencia corporativa para 500 equipos (computadoras, estaciones de trabajo, equipos móviles, servidores)</td><td>2 años</td></tr>
</table>
La solución de antivirus deberá proteger a todos los equipos informáticos (computadoras, estaciones de trabajo, equipos móviles y servidores) y cumplir con las siguientes especificaciones mínimas:

a) Solución antimalware
</td>
</tr>
</table>

	• La solución debe brindar protección por lo menos para los siguientes sistemas operativos: Windows 7/8/10/11; y para los siguientes sistemas operativos de servidor: Windows Server 2012, 2012 R2, 2016, 2019, 2022. • La solución debe brindar protección y gestionar dispositivos móviles con sistemas operativos Android y iOS, con funciones para protección de datos. • 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 las redes institucionales; y el segundo, cuando se conecte fuera. Los equipos deben poder actualizarse automáticamente desde el servidor o consola de administración de la solución, así como actualizarse directamente de los servidores del fabricante cuando se encuentren fuera de las redes institucionales • 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 desde la consola de administración o Escaneo de archivos basado en extensiones específicas o Escaneo basado en rutas específicas o Escaneo personalizado desde la consola de administración 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 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 opcionalmente a 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 opcionalmente 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 manejo debe estar integrado en la consola de administración de la solución. Análisis 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, puerto de origen; y dirección IP, 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. • La solución debe contar con tecnologías EDR que permitan identificar, detectar y prevenir amenazas avanzadas (APT). **b) Consola centralizada de administración** • 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. La consola de administración central deberá poder desplegar el licenciamiento a las demás consolas antivirus. • Se debe poder instalar por lo menos en plataformas Windows Server 2016, 2019 y 2022. • 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 descargar 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 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. **<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. **<u>Condiciones generales</u>** • 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 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.

- Kaspersky Total Security
- G Data Endpoint Protection Business

6. ANÁLISIS COMPARATIVO TÉCNICO

6.1. Descripción de métricas

Nº	Atributo	Descripción	Escala
	ATRIBUTOS INTERNOS		
1	Sistemas operativos de estaciones de trabajo	Microsoft Windows 7/8/10/11	5
2	Sistemas operativos de servidores	Microsoft Windows Server 2012, 2012 R2, 2016, 2019, 2022	5
3	Sistemas operativos de dispositivos móviles	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**

6.2. Puntajes

Nº	Atributo	Kaspersky Total Security	G Data Endpoint Protection Business
	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	4
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**	**97**

7. ANÁLISIS COMPARATIVO DE COSTO-BENEFICIO

- Producto: Kaspersky Total Security. Costo estimado: **S/ 35,872.00** (sobre la base de la cotización de BAFING S.A.C., tipo de cambio S/ 3.80: 8000x1.18x3.8)

- Producto: G Data Endpoint Protection Business. Costo estimado: **S/ 30,000.00** (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 evaluar que las condiciones económicas sean favorables para la entidad.

9. FIRMAS

OSINFOR
Firmado digitalmente por: ARTICA CUYUBAMBA Gustavo FAU 20522224783 soft
Motivo: En señal de conformidad
Fecha: 28/09/2023 17:34:10-0500

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

OSINFOR
Firmado digitalmente por: PRAELLI BUENO Juan Antonio FAU 20522224783 soft
Motivo: Soy el autor del documento
Fecha: 28/09/2023 16:43:53-0500

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

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/