"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la recuperación y consolidación de la economía peruana"

Anexo N° 01-B
ESPECIFICACIONES TÉCNICAS

Órgano y/o Unidad Orgánica:	UNIDAD FUNCIONAL DE TECNOLOGIAS DE LA INFORMACION	
Actividad del POI/Acción Estratégica PEI:	AOI00106600144. GESTIÓN OPERATIVA – UFTI 5000276	
Cuadro Multianual de Necesidades	Meta	0018
	Código Siga	140400030076
Denominación de la Contratación:	ADQUISICIÓN DE LICENCIAS DE SOFTWARE ANTIVIRUS PARA EL PROGRAMA DE EMPLEO TEMPORAL "LLAMKASUN PERÚ".	

I. FINALIDAD PÚBLICA

La presente adquisición tiene como finalidad lograr las metas y objetivos encargados al Programa de Empleo Temporal "LLamkasun Perú", por lo cual es necesaria la adquisición de software antivirus, que permitan garantizar la seguridad ante cualquier ataque de software malicioso a los equipos informaticos y servidores de producción del Programa de Empleo Temporal "LLamkasun Perú".

II. OBJETIVO DE LA CONTRATACIÓN

Adquirir licencias de software antivirus, a fin de brindar protección y seguridad a todo el sistema de red que conforma el Programa de Empleo Temporal "LLamkasun Perú" a nivel nacional, protegiendo los datos de las estaciones de trabajo, así como también los servicios que se brinda, tales como: Los sistemas de información, los sistemas de comunicación, sistemas de aplicaciones y sistemas de archivos, ante cualquier ataque de softwares maliciosos como: Virus, troyanos, macro virus, adware, apyware, gusanos, rootkits, ransomware y todo tipo de programa malicioso (malware).

III. CARACTERÍSTICAS TÉCNICAS:

EL Programa "LLamkasun Perú" requiere adquirir proyectores multimedia de acuerdo a las siguientes características:

ITEM	*DESCRIPCIÓN*	*CANTIDAD*	*UNIDAD DE MEDIDA*
01	*Licencias de software antivirus*	*530*	*Unidad*

- *El licenciamiento y la garantía integra será de doce (12) meses.*
- *470 licencias para pc y laptops*
- *56 licencias para servidores*
- *4 licencias para servidores con versiones legacy (Windows Server 2008 R2)*

3.1. CARACTERÍSTICAS Y CONDICIONES DEL BIEN

PERÚ MTPE
Firmado digitalmente por GUZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 20.10.2025 08:50:27 -05:00

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 17.10.2025 11:53:55 -05:00

Item	Atributos	Atributo Técnicos
ANTIVIRUS CORPORATIVO La entidad solicita una solución de software de un solo fabricante, una sola consola y un único agente que cubra con los requerimientos técnicos mínimos solicitados:		
Atributos Internos		
1	Sistemas operativos de estaciones de trabajo (en versiones de 32/64 bits	Microsoft Windows 10 Microsoft Windows 11 Microsoft Windows Server 2008, 2012, 2016 y 2019 Linux Mac
2	Protección y defensa frente a malware en portátiles, computadoras de escritorio	▪ La solución de seguridad para estaciones es de tipo integrada; es decir incluye un único agente que brinda protección frente a virus, spyware, adware, *rootkits,* comportamientos sospechosos, filtrado de seguridad URL, detección Web de ataques de Scripts maliciosos y aplicaciones potencialmente peligrosas en todos los protocolos de la red. ▪ La solución cuenta con una cuarentena de usuario final que permita controlar y/o autorizar el uso de ciertas aplicaciones no deseadas. ▪ La solución puede actualizarse (durante 12 meses) desde una consola centralizada y desde la web del fabricante simultáneamente con el fin de asegurar una completa protección aun cuando la consola central no se encuentre activa. ▪ La solución de seguridad instalada en todas las plataformas requeridas debe notificar los eventos de virus, spyware, adware, aplicaciones no deseadas, intrusiones, cambios en la configuración del cliente de seguridad a la consola central. ▪ El sistema de filtrado URL y el de detección Web de Ataques de Script maliciosos debe denegar el acceso al sitio y deber mostrar una página HTML de bloqueo en el navegador de internet (IE, Mozilla, Chrome, Opera, etc.) donde se indique el usuario y la razón por la que no ha podido acceder a dicha página. ▪ La solución deberá incluir un sistema para el Control de acceso web a sitios inapropiados. Este sistema deberá estar integrado al agente antimalware y deben permitir notificar o bloquear el acceso a sitio web en base a categorías. ▪ La solución para el Control de acceso a web a sitios inapropiados deberá incluir al menos 10 categorías de sitios web entre las que se encuentren principalmente Actividad Criminal, Armas, Contenido Ofensivo, Contenido para adultos, Juegos de Azar, Robo de Datos y Fraude, Programas Espía, Proxys anónimos, Violencia y Hackers. ▪ La solución permite la creación de CD, DVD o USB Booteables de emergencia mediante imágenes .ISO u otro formato de grabación de medios para la recuperación y limpieza de equipos infectados. La creación de dichas imágenes no deberá depender de productos de terceros ni requerir licenciamiento de productos adicionales al del propio fabricante. ▪ Detectar en tiempo real cualquier archivo infectado que trate de ser ejecutado, leído, copiado hacia/desde el servidor/estación de trabajo. El código malicioso debe ser detenido antes de que pueda propagarse por la red. La tecnología de esta solución le permitirá tomar muestras de posibles archivos maliciosos y enviarlas automáticamente para su análisis sin necesidad de intervención por parte del usuario. ▪ La solución ofertada incluirá alguna utilidad que realice un análisis detallado y a través del mismo reportar un

PERÚ MTPE
Firmado digitalmente por GUZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 20.10.2025 08:50:39 -05:00

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 17.10.2025 11:54:18 -05:00

		diagnostico profundo de la estructura del sistema, como librerías, aplicaciones instaladas, claves de registro entre otras, que puedan tener un comportamiento sospechoso como consecuencia del ataque de algún malware.
3	Anti-ransomware	▪ Protección de archivos contra ransomware ▪ Detección automática de archivos ▪ Protección de registros de arranque y disco
4	Firewall	▪ La solución incluye un firewall personal del mismo fabricante. ▪ El firewall personal es administrado centralizadamente desde la consola de gestión. ▪ El firewall permitirá bloquear, autorizar aplicaciones y puertos específicos tanto local como centralizadamente. ▪ El firewall deberá permitir trabajar en modo oculto. ▪ El firewall deberá permitir ser configurado en modo control o auditor con la finalidad de recoger información de aplicaciones, puertos y protocolos usados en el equipo de la red y que permite crear políticas de seguridad en forma rápida y simple. ▪ El firewall deberá reconfigurarse automáticamente con otro tipo de política de protección de acuerdo a la ubicación donde se encuentre. Esta política deberá realizarse mediante la detección de la MAC Address del Gateway de Red o del DNS
5	El sistema de prevención de intrusos de Host - HIPS y detección de desbordamiento de buffers (BOPS - Buffer Overflow Protection System)	▪ solución incluye una tecnología de detección de intrusos de host (HIPS) incorporado en el agente antimalware que brinde protección en acceso. ▪ La solución deberá incluir una tecnología para la detección de intentos de desbordamiento de buffers (SOPS - Buffer Overflow Protection System) incorporado en el agente antimalware. ▪ La solución deberá contar con una tecnología de prevención y detección de intrusos que detecta malware antes de su ejecución (pre-execution) y en ejecución (on-execution). ▪ El sistema HIPS está integrado en el agente antimalware y permite configurar en modo bloqueo de procesos o en modo solo alerta. ▪ El sistema HIPS no requiere ejecutar o instalar agentes o programas adicionales al motor antimalware ni ejecutarse en forma programada para la prevención y/o detección de intrusos de hosts.
6	Control de dispositivos	▪ Para la protección contra el malware en dispositivos externos, la solución incluye un sistema de control de dispositivos que detecta el uso de dispositivos USB, grabadores de CD/DVD, floppy disk, lectores de CD/DVD, HDD externos y dispositivos wireless. ▪ El sistema de control de dispositivos cuenta con opciones para permitir, bloquear, alertar y configurar en modo solo lectura los dispositivos indicados. ▪ El sistema de control de dispositivos permite la autorización de dispositivos específicos (basados en modelos específicos o marcas) la utilización de dispositivos cifrados e incluso contra el uso de interfaces de red como los módems convencionales y los módems 3G. ▪ El sistema de control de dispositivos estará integrado en el agente antimalware, es decir no requiere la instalación de programas adicionales en los equipos. ▪ El sistema de control de dispositivos cuenta con opciones para evitar el modo "puente-de-red'' para dispositivos de red wireless y módems, incluyendo los 3G, que permita evitar que los usuarios incumplan las políticas corporativas de acceso a internet.
7	Protección contra ataques de día cero	▪ La solución deberá contar con tecnologías de detección proactiva de amenazas conocidas y basadas en la nube (in the cloud) del mismo fabricante.

PERÚ MTPE

Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 20.10.2025 08:54:16 -05:00

PERÚ MTPE

Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 17.10.2025 11:54:32 -05:00

			▪ La solución ofertada deberá ofrecer una rápida y eficaz detección de archivos sospechosos mediante la comprobación instantánea de archivos sospechosos en la nube. ▪ El sistema de protección de filtrado URL realizando comprobaciones de direcciones web sospechosos (hackeadas, que albergan malware, etc.) en forma automática hacia la nube (base de datos del fabricante) para una rápida y efectiva protección contra este tipo de amenazas.
	8	Seguridad	▪ La solución debe ser capaz de evitar que sus procesos, servicios, archivos o archivos de registro puedan ser detenidos, deshabilitados, eliminados o modificados para de esta manera garantizar su funcionamiento ante cualquier tipo de ataque de virus. ▪ La solución deberá contar con medidas de seguridad para que el usuario de la estación de trabajo, sea este el administrador de la red o la PC no deje sin efecto políticas de seguridad corporativas. ▪ La desinstalación del módulo o cliente y sus componentes debe estar protegido con una clave de seguridad asignada por el administrador de la solución. Esta clave puede ser configurada para un grupo específico o todos los equipos en la red. ▪ La seguridad de la solución deberá integrarse al directorio activo de la red y el sistema de grupos de Microsoft para una mejor y efectiva protección. ▪ El usuario no podrá realizar una configuración particular a menos que el administrador de la red le otorgue privilegios ya sea localmente o mediante la integración con el Directorio Activo de Microsoft. ▪ La solución deberá contar con un sistema de administración de parches de múltiples fabricantes como Microsoft, Adobe, Mozilla, Apple y Citrix que permita conocer la lista de parches que no se han aplicado en los equipos administrados. ▪ La solución de administración de parches deberá mostrar además la lista de vulnerabilidades que son aprovechadas por atacantes o malwares específicos. ▪ Cualquier intento de vulneración de las características de seguridad deberá ser reportado a la consola de gestión centralizada
	9	Control de aplicaciones	▪ La solución debe contar con un sistema que permita controlar el uso de determinados tipos de aplicaciones en los equipos de la red. ▪ El sistema de control de aplicaciones debe permitir controlar y bloquear el uso de aplicaciones que causan un impacto negativo en el trabajo de los usuarios, en el uso del ancho de banda en la red y el incumplimiento de políticas corporativas las cuales se encuentran agrupadas o categorizadas por tipo de programas; al menos como Programas P2P, Mensajería Instantánea, Proxys, Herramientas de hacking, Control Remoto de Equipos y Máquinas Virtuales. ▪ La entidad puede solicitar al fabricante y/o postor la inclusión de nuevos programas y/o aplicaciones que considere que deben bloquearse y que se requiera incluir en dicho sistema.
	10	Control de acceso a la red	▪ La solución debe contar con la capacidad de integración con las políticas de seguridad de Cisco NAC. ▪ La solución incorpora un agente de control de acceso a la Red del mismo fabricante. Este agente también conocido como "Agente NAC" puede mantener todos los equipos sean estos administrados, no administrados o invitados

PERÚ MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 20.10.2025 08:54:45 -05:00

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 17.10.2025 11:54:40 -05:00

		(equipos que se conectan a la red esporádicamente) en buen estado y con la protección antivirus actualizado, así mismo, deberá asegurar que se corrijan las vulnerabilidades encontradas. ▪ El agente de control de acceso a la red permitirá establecer políticas para verificar al menos: ✓ Si el antivirus está activo y actualizado: ✓ Si el equipo cliente tiene activado el sistema de actualización de parches del sistema operativo ✓ Si el cliente firewall está activo. ✓ Si el equipo tiene activado algún sistema de encriptación de información. ▪ La solución NAC permite integrarse con el sistema DHCP de Microsoft para establecer políticas de control de acceso a la red.
11	Control de fuga de información (DLP	▪ La solución incluye un sistema para el control de fuga de datos conocido como DLP. ▪ El sistema de control de fuga de datos permite controlar, restringir y auditar la información que es copiada o enviada fuera de la red corporativa mediante el uso de dispositivos externos como USB, Internet, Correo Electrónico y Mensajería Instantánea. ▪ El sistema de control de fuga de datos debe ser del mismo fabricante y deberá poder controlar la información saliente por tipo de contenido y tipo de archivo ▪ El sistema de control de fuga de datos incluirá listas de control pre-configuradas para la elaboración rápida de políticas corporativas. ▪ La administración de este sistema se realiza desde la consola de administración central de la solución de seguridad antimalware.
12	Simulación de ataques phishing	▪ Deberá emula una variedad de tipos de ataques de phishing a través de campañas ▪ Contar con más de 490 plantillas de amenazas de correo electrónico ▪ Deberá generar informes automatizados sobre phishing y resultados de entrenamiento ▪ Deberá realizar capacitación a los usuarios a través de una capacitación ▪ Deberá importar usuarios, ya sea a través de un archivo CSV o utilizando herramienta de sincronización de Active Directory. ▪ Deberá contar con complemento de Outlook incluido proporciona a los usuarios la capacidad de informar sobre ataques simulados desde la bandeja de entrada ▪ deberá ser gestionado desde una sola consola
12	Encriptación de discos duros	▪ La solución incluye un sistema de encriptación de archivos y carpetas en el explorador de Windows, así como la encriptación de archivos adjuntos.
13	XDR	▪ Deberá detectar, investigar y responder a amenazas en sus diversas etapas, ▪ La solución deberá utilizar Inteligencia Artificial para Visualizar y Prevenir Incidentes de Seguridad ▪ Eliminar Vulnerabilidades. ▪ Mejorar la Seguridad. Detección de Amenazas ▪ las características EDR de protección de endpoint se entregan a través del mismo agente sin necesidad de instalar agentes adicionales ▪ Se podrá integrar con las herramientas de ciberseguridad que ya tiene la entidad ▪ Deberá obtener datos históricos en tiempo real y hasta 90 días.
Atributos Externos		

PERÚ MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 20.10.2025 08:54:53 -05:00

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 17.10.2025 11:54:50 -05:00

	14	Instalación y despliegue del software	▪ La instalación del software a las computadoras de los usuarios se puede realizar mediante: ✓ Instalación automática, mediante la sincronización con el Directorio Activo de Microsoft, ✓ Instalación remota desde la consola de administración ✓ Instalación manual mediante CD o recurso UNC. ▪ El instalador debe incorporar un Sistema de Eliminación de Software de Seguridad de Terceros (agentes antimalware y firewall) que permita desinstalar automáticamente otros productos de seguridad sin requerir realizar manualmente dicho proceso con el fin de optimizar el proceso de despliegue de la solución. ▪ La solución permite crear a pedido de la institución instaladores que permitan el despliegue del producto mediante CD o vía Web. Estos instaladores pueden ser personalizados y permitan por ejemplo contener información relativa a la propiedad de la institución. ▪ El Sistema de Eliminación de Software de Seguridad de Terceros debe ser del mismo fabricante. ▪ El Sistema de Eliminación de Software de Seguridad de Terceros está incorporado en el sistema de instalación del agente antimalware es decir puede activarse o desactivarse al momento del despliegue de la solución. ▪ El instalador permite la instalación del agente de Control de Acceso a la Red durante el despliegue de la solución.
	15	Actualización de firma y nuevas versiones de producto	▪ Las actualizaciones se realizarán automáticamente (programadas) y manualmente del fichero de firmas de virus y del motor de escaneado del malware en las estaciones de trabajo desde internet. ▪ La actualización de firmas automáticas deberá realizarse cada 30 minutos o menos. ▪ El tamaño de las actualizaciones de firmas de virus es pequeño de tal modo que no tenga un impacto negativo en el tráfico de la red (máximo 100 Kb por actualización). ▪ La actualización de nuevas versiones del producto se puede realizar automáticamente y no requiere la desinstalación y/o reinstalación de algún componente previo, estas actualizaciones son increméntales. ▪ La solución permite programar la comprobación de nuevas versiones de la solución al menos 12 horas y programar la instalación automática de ellas en horas de menos tráfico de red. Para este fin, la solución debe contar con opciones para la programación del horario por día y hora especificada.
	16	Consola de administración en la nube	▪ La solución deberá contar con una consola de administración en la nube, desde donde pueda administrar y controlar todos los componentes de la solución ofertada en forma centralizada y distribuida. ▪ La herramienta deberá tener incluido la capacidad de gestión de las políticas de control de acceso a la red sin requerir instalar productos adicionales. ▪ La consola debe permitir la administración simultáneamente de equipos Windows. ▪ La herramienta deberá ser escalable y debe permitir la administración de complejas redes, permitiendo la administración centralizada y distribuida de más de 100 equipos desde una sola consola ▪ La consola debe sincronizarse con el Directorio Activo para la instalación automática de la solución de seguridad en los equipos. ▪ La administración deberá estar basada en políticas y deberá contener al menos Actualización, Opciones Antimalware, HIPS, Control de Aplicaciones, Control de Dispositivos, Control de Fuga de Datos, NAC y Firewall.

PERÚ MTPE

Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 20.10.2025 08:55:02 -05:00

PERÚ MTPE

Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 17.10.2025 11:54:59 -05:00

			▪ Cualquier cambio en las políticas deberán desplegarse automáticamente a los equipos sean estos Windows. ▪ Debe contar con filtros de control que permitan detectar de forma rápida los equipos no protegidos o los que no cumplen con las políticas de seguridad. ▪ El administrador deberá poder crear políticas desde la consola para evitar el uso de aplicaciones no deseadas, así como eliminar, autorizar y limpiar las mismas en los clientes. ▪ La consola deberá poder utilizar al menos 3 tipos diferentes de mecanismos para detectar equipos en la red (TCP/IP, Active Directory y otros) ▪ Se deberá poder crear políticas de actualización para equipos con conexión lenta pudiendo limitarse el ancho de banda utilizado durante las actualizaciones. ▪ La consola deberá ser capaz de determinar equipos que cumplan con las políticas centrales y/o fueron modificadas localmente. Eventualmente deberá poder "forzar" a los equipos a cumplir con las políticas centrales con tan solo un Click. ▪ La consola debe Permitir obtener una visibilidad clara de todos sus usuarios, sus dispositivos y su estado de protección. ▪ La consola deberá contar con un sistema de reportes y mecanismos de notificación de eventos vía correo electrónico. ▪ La consola deberá almacenar un histórico de eventos de cada equipo administrado pudiéndose conocer también el nombre del equipo, descripción, SO, Service Pack, IP, Grupo, última actualización, eventos de error, etc. desde la consola. ▪ La consola deberá administrar el sistema de prevención contra intrusiones de host (HIPS) y el sistema de protección contra desbordamiento de buffers (BOPS) como políticas de seguridad. ▪ La consola deberá permitir delegar la administración basada en roles y ubicaciones geográficas, permitiendo de esta forma delegar la administración por áreas geográficas manteniendo de esta forma el control de la seguridad corporativa. ▪ El sistema para la delegación de roles deberá contener un administrador de permisos, pudiendo crear distintos perfiles con permisos particulares para cada administrador. ▪ La consola deberá permitir crear excepciones para el control de dispositivos (control total, solo lectura y bloqueo) y filtro web (por nombre de dominio, dirección IP y dirección IP con mascará de subred) para un grupo particular de equipos o toda la red. ▪ Debe incluir la capacidad para la desinfección y limpieza remota de adware/aplicaciones potencialmente peligrosas, así como también de virus, troyanos, gusanos, rootkits y spyware. ▪ La consola deberá permitir acceder a un sistema de visualización y búsqueda de eventos para las políticas de control de aplicaciones, dispositivos, fuga de datos y firewall. ▪ La consola deberá tener integrada un visor de parches con la finalidad de que el administrador de la solución pueda verificar la lista de parches que faltan aplicar en los equipos administrados, así como conocer la cantidad de equipos a los cuales falta aplicar un determinado parche. ▪ La consola deberá tener integrado un visor para el control web el cual deberá permitir visualizar los sitios web a los cuales los usuarios han intentado ingresar en contra las políticas de seguridad de la empresa. ▪ Desde el sistema de visualización y búsqueda de eventos se podrá crear excepciones y nuevas reglas a las políticas de

PERÚ MTPE

Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 20.10.2025 08:55:13 -05:00

PERÚ MTPE

Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 17.10.2025 11:55:10 -05:00

		control de dispositivos y cortafuegos previamente establecidas respectivamente. ▪ La consola debe de permitir realizar un backup, de todas las bases de datos y configuraciones realizadas en el sistema, sin necesidad de detener los servicios
17	Administración de licencias	▪ La solución deber permitir el manejo flexible de las licencias, de manera que puedan ser reasignadas en caso de cambie de equipos
Atributos de Uso		
18	Alertas y Reportes	▪ La solución deberá ser capaz de notificar los eventos de virus a través de diferentes medios (correo electrónico, alerta de registros, etc.) ▪ La solución deberá generar reportes gráficos, imprimibles y exportables de la cobertura de versiones, actualizaciones e infecciones. ▪ La solución deberá contener un sistema de reportes que permitir ver el estado de la protección de la red en línea. Este sistema debe mostrar en tiempo real lo que está ocurriendo en la red. ▪ La solución deberá permitir acceder a reportes basados en el usuario que permita conocer rápidamente el cumplimiento de políticas por cada usuario. ▪ La solución deberá incorporar un sistema de reportes que permita programar la creación y envió de reportes en formato PDF y HTML vía correo electrónico en una determinada hora y fecha de día. ▪ La solución deberá incorporar un mecanismo de conexión con la base de datos para la creación de reportes personalizados y directos a la base de datos.
19	Soporte técnico	▪ La solución debe contar con soporte técnico 8x5 escalable hacia la casa matriz incluido en la licencia y en español. ▪ El postor deberá contar con al menos 01 especialista certificado por el fabricante en el área de antivirus. ▪ El postor capacitara a un mínimo de 08 horas en las herramientas administrativas del software dictado y certificado por el postor, para 2 personas como mínimo. ▪ El postor deberá brindar el servicio de instalación, configuración y pruebas del aplicativo antivirus en el 50% de equipos de la institución. ▪ El postor tendrá 05 días calendario para realizar la implementación del software señalado líneas arriba contabilizados desde el día siguiente de la entrega del software.

INSTALACIÓN Y/O CONFIGURACIÓN

- *En las oficinas del Programa de Empleo Temporal "LLamkasun Perú" sito: Av. Salaverry N° 655, 7° Piso, Edificio del Ministerio de Trabajo y Promoción del Empleo, Jesús María.*
- *La solución deberá garantizar la protección de todas las pc y servidores de la entidad independientemente que sean físicos y virtuales.*

SOPORTE TÉCNICO

- *Se brindará durante el periodo de garantía de doce (12 meses) en la modalidad 24x7x365 incluido domingos y feriados, contabilizadas a partir del día siguiente de emitida la conformidad de entrega de bienes.*
- *El plazo máximo para acudir al local del Programa de Empleo Temporal "LLamkasun Perú", identificar las causas del incidente y ejecutar la solución al primer nivel, será de cuatro (04) horas.*
- *El soporte será ON–SITE y/o ON-LINE y atenderán incidentes relacionados al software, orientación técnica o atender requerimientos técnicos durante cualquier día de la semana.*
- *El PROVEEDOR debe contar con el servicio de recepción de incidentes 24x7x365 incluido domingos y feriados, a través de llamadas y de correos, para lo que deberá brindar; un número directo y una*

PERÚ MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 20.10.2025 08:55:23 -05:00

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 17.10.2025 11:55:19 -05:00

dirección de correo electrónico el cual será utilizado por el Programa de Empleo Temporal "LLamkasun Perú" para reportar las averías.

- *El soporte técnico comprenderá la solución de antivirus y antimalware, cualquier tipo de problema, incidente o avería a una interrupción parcial o total referido a la solución.*
- *El soporte técnico comprenderá la instalación de parches, actualizaciones, nuevas versiones, vacunas, reglas, filtros, releases, bases de datos de firmas de virus, de la solución ofertada antivirus y antimalware y sus reparaciones (parches, fixes).*
- *El soporte técnico incluye el análisis, actualización, corrección y documentación de problemas en la solución implementada.*
- *Deberá brindar soporte técnico In Situ a cargo de expertos profesionales en análisis de virus, malware y ransomware, el cual lo asistirá en forma personal. Se precisa, que el soporte técnico In Situ de dará en caso de fallas que no puedan ser solucionadas de manera remota.*
- *El proveedor deberá asegurar que la solución completa quede operativa y en óptimas condiciones de seguridad y performance, y restaurar a estos su funcionamiento normal cuando una falla se reproduzca.*
- *El proveedor deberá proporcionar, sin costo adicional para la Institución cualquier complemento que no haya sido descrito en su propuesta técnica y cuya ausencia determine la imposibilidad de cumplir con lo solicitado como parte de soporte técnico.*
- *El proveedor deberá de ejecutar como mínimo una revisión mensual con la finalidad de asegurar el correcto funcionamiento de la solución implementada.*
- *El proveedor deberá de realizar en forma mensual el análisis y verificación de la seguridad en la red de la entidad.*
- *El proveedor deberá de aplicar de forma proactiva políticas de seguridad en la consola de administración del antivirus que permitan un mejor control en la red de trabajo del Programa.*

CAPACITACIÓN Y/O ENTRENAMIENTO

- *Se brindará capacitación y certificado oficial de la marca ofertada por el postor, para dos (02) colaboradores de la Unidad Funcional de Tecnologías de la Información.*

IV. REQUISITOS DEL PROVEEDOR

- Registro Único del Contribuyente (RUC) vigente, actividad económica de acuerdo al objeto de la contratación.
- Registro Nacional de Proveedores (RNP) vigente - bienes, de corresponder.
- No encontrarse inhabilitado ni suspendido para contratar con el Estado.
- Documento que acredite la garantía ofertada, acreditado mediante certificado de garantía, carta de garantía y/o declaración jurada.
- Deberá ser miembro del FIRST, lo deberá acreditar con una copia simple.
- Deberá contar con la ISO 27001:2022 - Gestión de la seguridad de la información.

4.1 Requisitos del Postor

- *Registro Único del Contribuyente (RUC) vigente, actividad económica de acuerdo al objeto de la contratación.*
- *Registro Nacional de Proveedores (RNP) vigente - bienes, de corresponder.*
- *No encontrarse inhabilitado ni suspendido para contratar con el Estado.*
- *Experiencia mínima de tres (03) ventas relacionadas a la contratación, el mismo que debe estar acreditado con orden de compra, factura, comprobante de pago u otro documento que lo acredite. Se considera como similares la venta de soluciones de antimalware avanzado.*
- *Contar con una mesa de ayuda propia para brindar el soporte 24x7x365 incluidos domingos y feriados, el cual debe ser acreditada a través de declaración jurada.*
- *El postor debe ser representante acreditado en el país o canal autorizado para la distribución o venta de productos del fabricante, subsidiaria o su representante de los bienes ofertados. Se podrá sustentar con carta de fabricante y/o documento que acredite su condición de partner*

4.2 Requisitos del Personal

a) Dos (02) Especialistas de Soporte Técnico e Implementación:

MTPE

Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 20.10.2025 08:55:32 -05:00

MTPE

Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 17.10.2025 11:55:30 -05:00

- *El especialista, ingeniero y/o técnico en las carreras de sistemas y/o computación e informática y/o electrónica y/o Telecomunicaciones y/o afines.*
- *Contar certificación oficial vigente otorgada por el fabricante del producto ofertado y deberán estar capacitados en el manejo, instalación, configuración y administración de la solución antivirus ofertada*
- *Deberá contar con una experiencia como mínima de tres (03) años en implementaciones de soluciones antivirus de endpoint y soluciones de seguridad perimetral, la cual deberá ser acreditada fehacientemente mediante constancias, certificados, contratos y/u otro documento que lo acredite.*

Se podrá acreditar las certificaciones de los especialistas a cargo, presentando copias simples en idioma original

V.	**REGLAMENTOS TÉCNICOS, NORMAS METROLÓGICAS Y/O SANITARIAS**
	NO APLICA
VI.	**SEGURO**
	NO APLICA
VII.	**PRESTACIONES ACCESORIAS**
	NO APLICA
VIII.	**LUGAR Y PLAZO DE ENTREGA**
	LUGAR: En el almacén de las instalaciones del Programa Llamkasun Perú, Av. Salaverry N° 655, Piso 7, Edificio del Ministerio de Trabajo y Promoción del Empleo, Jesús María. La entrega se efectuará previa coordinación con el responsable de Almacén o quien haga sus veces del Programa Llamkasun Perú. El horario de recepción es de lunes a viernes de 9:00 horas a 17:00 horas, teniendo en cuenta que el horario de refrigerio es de las 13:00 horas a 14:00 horas. **PLAZO:** El plazo de entrega será de hasta siete (07) días calendarios, contabilizados a partir del día siguiente de la notificación de la Orden de Compra
IX.	**ENTREGABLES**
	NO APLICA
X.	**CONFORMIDAD**
	La conformidad de los bienes adquiridos será emitida por la Unidad Funcional de Tecnologías de la Información, cuyo contenido será el cumplimiento de cada punto del bien descrito.
XI.	**FORMA Y CONDICIONES DE PAGO**
	El Pago del 100% de los bienes se efectuará mediante cuenta CCI, en una armada, previa conformidad emitida por la Unidad Funcional de Tecnologías de la Información del Programa "Llamkasun Perú" con V°B° del jefe y/o quien haga sus veces. Para efectos del pago de los bienes entregados, el contratista deberá de presentar la siguiente documentación: • Documento de recepción de almacén (guía de remisión con recepción de almacén) • Comprobante de pago actualizado • Conformidad del área usuaria • Documento que acredite la garantía ofertada • Carta del CCI El contratista tendrá hasta tres (03) días calendario de culminado el plazo de entrega para presentar la documentación solicitada.

PERÚ MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 20.10.2025 08:55:42 -05:00

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 17.10.2025 11:55:44 -05:00

XII.	**GARANTÍAS**
	Se establece una garantía mínima de doce (12) meses, contados a partir de la fecha de conformidad de los bienes. El PROVEEDOR, proporcionará una garantía de doce (12) meses por el bien adquirido; dicha garantía iniciará al día siguiente de emitida la conformidad por la puesta en funcionamiento de las licencias de software antivirus.
XIII.	**CONFIDENCIALIDAD**
	• El Contratista se obliga a guardar reserva absoluta en el manejo de información y documentación a la que se tenga acceso relacionado con la prestación, quedando expresamente prohibido revelar dicha información a terceros. El proveedor, deberá dar cumplimiento a todas las políticas y estándares definidos por la Entidad, en materia de seguridad de la información. • Dicha obligación comprende la información que se entrega como también la que se genera durante la realización de las actividades y la información producida una vez que se haya concluido con la prestación y/o entrega del bien y/o servicio. • Dicha información puede consistir en mapas, dibujos, fotografías, mosaicos, planos, informes, recomendaciones, cálculos, documentos y demás documentos e información compilados o recibidos por el contratista. • El Contratista cederá en forma exclusiva al Programa los títulos de propiedad, derechos de autor y otro tipo de derecho de cualquier naturaleza sobre cualquier material producido bajo las estipulaciones de la presente especificación técnica.
XIV.	**GASTOS POR DESPLAZAMIENTO**
	No aplica.
XV.	**RESPONSABILIDAD DEL PROVEEDOR**
	El proveedor es responsable por el correcto traslado de los bienes, garantizando la integridad de los mismos.
XVI.	**PENALIDAD POR MORA**
	Penalidad por Mora en la ejecución de la prestación: En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la entidad contratante le aplica automáticamente una penalidad por mora por cada día de atraso que le sea imputable. La penalidad se aplica automáticamente y se calcula de acuerdo con la siguiente fórmula: $\text{Penalidad diaria} = \frac{0.10 \times \text{monto}}{F \times \text{plazo}}$ Donde F tiene los siguientes valores: Para bienes y Servicios: F = 0.40 Para obras: a) Para plazos menores o iguales a sesenta días: F = 0.40 b) Para plazos entre sesenta y uno a ciento veinte días: F = 0.25. c) Para plazos mayores a ciento veinte días: F = 0.15 Para consultoría de Obras: a) Para plazos menores o iguales a sesenta días: F = 0.40. b) Para plazos mayores a sesenta días: F = 0.25.

MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 20.10.2025 08:55:52 -05:00

MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 17.10.2025 11:55:58 -05:00

Tanto el monto como el plazo se refieren, según corresponda, al monto vigente del contrato, componente o ítem que debió ejecutarse o, en caso de que estos involucren entregables cuantificables en monto y plazo, al monto y plazo del entregable que fuera materia de retraso.

Nota:

Asimismo, es de indicar que cualquier tipo de penalidad a aplicar puede alcanzar como máximo un monto equivalente al diez por ciento (10%) por cada entregable, del monto total del contrato vigente y/o de la orden de compra.

XVII. OTRAS PENALIDADES

No aplica.

XVIII. RESOLUCION CONTRACTUAL

Son las establecidas en el Artículo 68 de la Ley General de Contrataciones N° 32069:

a) Caso fortuito o fuerza mayor que imposibilite la continuación del contrato.
b) Incumplimiento de obligaciones contractuales, por causa atribuible a la parte que incumple.
c) Hecho sobreviniente al perfeccionamiento del contrato, de supuesto distinto al caso fortuito o fuerza mayor, no imputable a ninguna de las partes, que imposibilite la continuación del contrato.
d) Por incumplimiento de la cláusula anticorrupción.
e) Por la presentación de documentación falsa o inexacta durante la ejecución contractual.
f) Configuración de la condición de terminación anticipada establecida en el contrato, de acuerdo con los supuestos que se establezcan en el reglamento para su aplicación.

XIX. CLAUSULA ANTICORRUCION Y ANTISOBORNO

EL CONTRATISTA declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o entrega de cualquier beneficio o incentivo ilegal, de manera directa o indirecta, a los evaluadores del proceso de contratación o cualquier servidor de la entidad contratante.

Asimismo, EL CONTRATISTA se obliga a mantener una conducta proba e íntegra durante la vigencia del contrato, y después de culminado el mismo en caso existan controversias pendientes de resolver, lo que supone actuar con probidad, sin cometer actos ilícitos, directa o indirectamente.

Aunado a ello, EL CONTRATISTA se obliga a abstenerse de ofrecer, negociar, prometer o dar regalos, cortesías, invitaciones, donativos o cualquier beneficio o incentivo ilegal, directa o indirectamente, a funcionarios públicos, servidores públicos, locadores de servicios o proveedores de servicios del área usuaria, de la dependencia encargada de la contratación, actores del proceso de contratación y/o cualquier servidor de la entidad contratante, con la finalidad de obtener alguna ventaja indebida o beneficio ilícito. En esa línea, se obliga a adoptar las medidas técnicas, organizativas y/o de personal necesarias para asegurar que no se practiquen los actos previamente señalados.

Adicionalmente, EL CONTRATISTA se compromete a denunciar oportunamente ante las autoridades competentes los actos de corrupción o de inconducta funcional de los cuales tuviera conocimiento durante la ejecución del contrato con LA ENTIDAD CONTRATANTE.

Tratándose de una persona jurídica, lo anterior se extiende a sus accionistas, participacioncitas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o cualquier persona vinculada a la persona jurídica que representa; comprometiéndose a informarles sobre los alcances de las obligaciones asumidas en virtud al contrato.

PERÚ MTPE

Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 20.10.2025 08:56:01 -05:00

PERÚ MTPE

Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 17.10.2025 11:56:13 -05:00

	Finalmente, el incumplimiento de las obligaciones establecidas en esta cláusula, durante la ejecución contractual, otorga a LA ENTIDAD CONTRATANTE el derecho de resolver total o parcialmente el contrato. Cuando lo anterior se produzca por parte de un proveedor adjudicatario de los catálogos electrónicos de acuerdo marco, el incumplimiento de la presente cláusula conllevará que sea excluido de los Catálogos Electrónicos de Acuerdo Marco. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar.
XX.	**APLICACIÓN SUPLETORIA**
	Según Ley Nº 32069, Ley General de Contrataciones Públicas y su Reglamento, Código Civil Peruano, entre otras normativas vigentes.
XXI.	**MEDIDAS DE SEGURIDAD**
	No aplica.
XII.	**GESTION DE RIESGO**
	Según Literal C) del Artículo 60 de la Ley General de Contrataciones Públicas N° 32069
XIII.	**SOLUCION DE CONTROVERSIAS**
	Todos los conflictos que se deriven de la ejecución e interpretación de la presente contratación son resueltos mediante trato directo, conciliación y/o acción judicial.
XIV.	**CLÁUSULA DE CUMPLIMIENTO DE ACUERDO A LO ESTABLECIDO EN LA LEY N° 31564**
	Son causales de resolución de contrato la presentación con información inexacta o falsa de la Declaración Jurada de Prohibiciones e Incompatibilidades a que se hace referencia en la Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público. Asimismo, en caso se incumpla con los impedimentos señalados en el artículo 5 de dicha ley se aplicará la inhabilitación por cinco años para contratar o prestar servicios al Estado, bajo cualquier modalidad".

Solicitado por:

PERÚ MTPE
Firmado digitalmente por GUIZADO CASTILLO Jose Manuel FAU 20504007945 hard
Motivo: Soy el autor del documento
Fecha: 20.10.2025 08:56:12 -05:00

Firma del jefe del Área Usuaria

PERÚ MTPE
Firmado digitalmente por VELASQUEZ FLORES Juan Pablo FAU 20504007945 hard
Motivo: Doy V° B°
Fecha: 17.10.2025 11:56:25 -05:00