Sistema Integrado de Gestion Administrativa
Modulo de Logistica

SOLICITUD DE COTIZACION

UNIDAD EJECUTORA : 312 GOB.REG.DPTO.CUSCO - UGEL CUSCO
NRO.IDENTIFICACION : 1644

Señores :

R.U.C :

Dirección :

Teléfono :

CCMN :

Concepto ADQUISICIÓN DE LICENCIAS PARA LOS EQUIPOS DE COMPUTO ESTACIONARIAS Y LICENCIAS DE SEGURIDAD AVANZADA ENDPOINT DETECTION Y RESPONSE (EDR) PARA LOS EQUIPOS DE COMPUTO TIPO SERVIDOR DE LA UNIDAD DE GESTIÓN EDUCATIVA LOCAL CUSCO

CANTIDAD REQUERIDA	UNIDAD MEDIDA	DESCRIPCIÓN	PRECIO UNITARIO	PRECIO TOTAL
116	UNIDAD	SOFTWARE ANTIVIRUS		
5	UNIDAD	SOTWARE(INC. LICENCIA) ANTIVIRUS PARA SERVIDOR		
		SEGÚN ESPECIFICACIONES TÉCNICAS ADJUNTO		
SON:			TOTAL	

Las cotizaciones deben estar dirigidas a la Unidad de Gestion Educativa Local del Cusco en la siguiente direccion: Av.Camino Real N° 114 -Wanchaq - Cusco

Condiciones del bien o servicio (*) obligatorio

*Forma de pago :

*La cotizacion incluye IGV :

*Plazo de entrega/ejecucion del servicio :

*Tipo de moneda :

*Validez de la cotizacion :

*Fecha :

Remitir junto a la cotizacion la declaracion jurada y carta de autorizacion debidamente firmada y sellada.

OFICINA DE ABASTECIMIENTO

FIRMA Y SELLO DEL PROVEEDOR

ESPECIFICACIONES TECNICAS

ADQUISICIÓN DE LICENCIAS ANTIVIRUS PARA LOS EQUIPOS DE CÓMPUTO ESTACIONARIAS Y LICENCIAS DE SEGURIDAD AVANZADA ENDPOINT DETECTION & RESPONSE (EDR) PARA EQUIPOS DE CÓMPUTO TIPO SERVIDOR DE LA UNIDAD DE GESTIÓN EDUCATIVA LOCAL DEL CUSCO

1. DEPENDENCIA SOLICITANTE	Equipo de Informática – Unidad de Gestión Educativa Local Cusco.
2. OBJETO DE LA ADQUISICION	El presente requerimiento tiene por objeto la adquisición de licencias de software antivirus para los equipos de cómputo estacionarios y licencias de seguridad avanzada tipo Endpoint Detection & Response (EDR) para los equipos de cómputo tipo servidores de la Unidad de Gestión Educativa Local Cusco, con la finalidad de fortalecer la protección, detección y respuesta ante incidentes de seguridad informática dentro de la infraestructura tecnológica institucional. La adquisición comprende la provisión, instalación, configuración y activación de las licencias de seguridad digital mencionadas, que deberán ser compatibles con los sistemas operativos y plataformas tecnológicas implementadas en la UGEL Cusco, garantizando su correcto funcionamiento en los entornos de red local y servidores institucionales. Asimismo, el proveedor deberá proporcionar asistencia técnica y soporte durante la vigencia de las licencias, incluyendo actualizaciones automáticas de definiciones de amenazas y mantenimiento de la plataforma de administración centralizada, a fin de asegurar la protección continua y la gestión integral de los equipos de cómputo y servidores institucionales.
3. FINALIDAD PÚBLICA	La presente adquisición tiene por finalidad garantizar la continuidad operativa, la seguridad y la integridad de la información institucional de la Unidad de Gestión Educativa Local Cusco, mediante la implementación de soluciones de protección antivirus para equipos de cómputo estacionarios y licencias de seguridad avanzada Endpoint Detection & Response (EDR) para los servidores institucionales. Esta medida busca prevenir, detectar y responder eficazmente ante amenazas cibernéticas, ataques de malware, ransomware y accesos no autorizados, asegurando el correcto funcionamiento de los sistemas informáticos críticos utilizados en la gestión administrativa, financiera, pedagógica y de recursos humanos, tales como el Sistema Integrado de Gestión Administrativa (SIGA), Sistema Único de Planillas (SUP), SIAF, Nexus, Mesa de Partes Virtual, entre otros. De esta manera, la adquisición contribuye directamente al fortalecimiento de la ciberseguridad institucional y al

	cumplimiento de los lineamientos establecidos en la Política Nacional de Transformación Digital y el Decreto Supremo N.° 029-2021-PCM, que promueven la protección de los activos digitales del Estado y la gestión segura de la información pública. Asimismo, la implementación de estas soluciones tecnológicas permitirá preservar la disponibilidad, confidencialidad y trazabilidad de los datos institucionales, asegurando la eficiencia y continuidad de los servicios públicos que brinda la UGEL Cusco a la comunidad educativa de su jurisdicción, contribuyendo así al uso responsable y sostenible de los recursos tecnológicos del Estado.
4. VINCULACIÓN AL POI	La presente adquisición permitirá el cumplimiento de las actividades en forma normal y operativa del trabajo programado en el POI en la actividad operativa **C0083 – ESTABLECER ESTRATEGIAS DE PERMANENTE TRANSFORMACIÓN A FIN DE MEJORAR LOS SERVICIOS ADMINISTRATIVOS DE LA ENTIDAD ORIENTADO A RESULTADOS**.
5. CARACTERISTICAS DEL BIEN	**CANTIDAD DE LICENCIAS ANTIVIRUS** **RESUMEN** **TOTAL COMPUTADORAS - LAPTOP**: 116 **TOTAL SERVIDORES**: 5 **ESPECIFICACIONES TÉCNICAS** **SOLUCIÓN DE PROTECCIÓN PARA EQUIPOS DE CÓMPUTO ESTACIONARIOS.** a. La solución (en su última versión) deberá ser compatible con los siguientes sistemas operativos: Microsoft® Windows® 11/10.Ubuntu Desktop 18.04 y superior x64, RedHat para Desktop 7, 8 x64 y superior, SUSE Linux Enterprise Desktop 15 x64 y superior. Apple macOS 10.12 y superior. b. El producto ofertado debe contar con un módulo de detección en tiempo real que proteja contra códigos maliciosos en cada ejecución, uso o creación de archivos en el equipo. c. El producto ofertado debe contar con un sistema de detección de intrusos que realice un análisis de contenido del tráfico de red y además permita proteger de ataques haciendo que cualquier tráfico dañino sea bloqueado. d. El producto ofertado deberá permitir realizar un escaneo del equipo en modo seguro bajo línea de comando donde se podrá especificar las opciones para la limpieza de virus. e. La solución es capaz de detectar todo tipo de amenazas, entre los más comunes: virus, gusanos, troyanos, spyware, adware, rootkits, bots, ransomware, etc. f. La solución deberá contar con una funcionalidad antiransomware. g. El producto ofertado debe contar con la funcionalidad de evitar que el malware dañe o deshabilite la protección antivirus, por lo que se puede estar seguro de que el sistema permanece protegido constantemente. h. El programa antivirus debe contar con la opción de crear análisis bajo demanda. Estos análisis se podrán configurar para realizarse inmediatamente o a una fecha y hora futura, y también se podrán

	configurar para realizarse una vez o repetirse a diferentes intervalos, días, semanas, meses, etc. i. Debe permitir elegir las unidades a escanear para los escaneos bajo demanda. j. El producto ofertado debe ser capaz de crear exclusiones de escaneo ya sea por archivo, extensión o carpeta específica. k. El producto ofertado debe pedir una contraseña ante intentos de cambio indebidos en la configuración del producto. l. El cliente antivirus debe tener un agente que le permita ser administrado desde una consola centralizada. Este agente debe reportar el estado de todas las soluciones antivirus instaladas en la dependencia. m. El producto ofertado deberá permitir generar dentro de la misma solución antivirus repositorios de actualización, los cuales deberán ser distribuidas mediante protocolo http localmente, sin depender de aplicaciones externas o de tareas desde la consola de Administración. n. El producto ofertado debe tener una funcionalidad en donde todas las ventanas emergentes se deshabiliten y la protección del sistema seguirá ejecutándose en segundo plano, pero no requerirá ninguna interacción por parte del usuario. o. El producto ofertado deberá tener una funcionalidad de catalogar a los procesos de los equipos de acuerdo con la reputación basada en la nube. Esta permitirá recopilar información anónima del ordenador afectada con las amenazas detectadas recientemente. p. La solución debe tener sistema de prevención de intrusiones basado en el host, (HIPS). q. El sistema HIPS debe tener los siguientes modos de configuración: automático, inteligente, interactivo, basado en políticas y aprendizaje. r. El producto ofertado permitirá crear grupos que contengan varios vínculos URL para crear reglas de permiso y bloqueo a determinados sitios web. s. El producto ofertado deberá analizar protocolos de e-mail POP3, IMAP, MAPI. t. La protección del correo electrónico en el cliente debe permitir definir si se desea escanear sólo correo recibido, correo enviado o correo leído. u. El producto ofertado debe tener la capacidad de añadir una nota o etiqueta en los correos electrónicos recibidos o leídos. v. La solución deberá contar con un módulo de protección Anti-Phishing que detecte sitios fraudulentos y bloquee el acceso total, evitando que los usuarios ingresen cualquier tipo de información. w. El producto ofertado debe tener un módulo de protección en tiempo real para el acceso a la web. x. El producto ofertado debe ser capaz de escanear a través del protocolo SSL (HTTPS), de manera que se pueda impedir la descarga de archivos infectados. y. El producto ofertado debe de permitir realizar exclusiones de URL para que no sean analizadas por el antivirus tanto en el protocolo HTTP, y HTTPS. z. El producto ofertado debe tener un Módulo de control de dispositivos que permita acceso de solo lectura, lectura/escritura o bloquear dispositivos de acuerdo con una lista predefinida que incluya como mínimo: dispositivos USB, CD-ROM y dispositivos Bluetooth o módems. aa. El producto ofertado debe tener un módulo de control de dispositivos que permita crear varios grupos de dispositivos donde se podrán aplicar reglas distintas y además permitirá detectar los dispositivos conectados a la PC y agregarlos al listado de grupo de dispositivos.

	Además, incluye la funcionalidad de aplicar esta regla por un período de tiempo determinado (hora y días). bb. El producto ofertado debe ser capaz de crear CD's, ISO's o USB de rescate, que permitan escanear los equipos Microsoft. cc. El producto debe contar con una primera exploración automática después de la instalación del programa, lo que permite asegurar que el equipo se encuentra protegido desde el comienzo. dd. El producto debe permitir realizar exploraciones completas mientras el equipo no está en uso, es decir que realice el escaneo cuando el equipo se encuentre bloqueado o suspendido. Esto con la finalidad de obtener un mejor rendimiento y limpieza del sistema. ee. El producto ofertado debe contar con una herramienta que permita examinar a fondo el ordenador, y con esta información poder ayudar a determinar la causa de un comportamiento sospechoso en el equipo que pueda deberse a una infección de malware o incompatibilidad de software o hardware. La información para recopilar deberá ser detallada sobre los componentes del sistema (como los controladores, aplicaciones instaladas, conexiones de red o entradas importantes del registro). ff. La solución deberá poder realizar exploraciones en estado inactivo para poder brindar de esa forma, una protección proactiva mientras el equipo no está en uso. gg. La solución deberá contar con la funcionalidad de bloqueo de exploits, que evite la explotación de vulnerabilidades en las aplicaciones. hh. La solución deberá contar con un modo transparente de uso, en el cual no muestre ninguna alerta cuando se esté ejecutando una aplicación en pantalla completa. ii. La solución deberá contar con módulo de exploración avanzada de memoria que permita detectar las amenazas más sofisticadas que están diseñadas para evadir la detección a través de mecanismos tradicionales. jj. El producto debe tener un control web para limitar el acceso a los sitios web por categoría o bien una categoría de sitios web, además de poder mostrar al usuario una notificación de bloqueo. kk. La solución deberá contener dentro del módulo de firewall la funcionalidad de bloqueo de exploits, que evite la explotación de vulnerabilidades en las aplicaciones. ll. La solución de antivirus debe ejecutar un escaneo o exploración de cualquiera de los siguientes estados en la computadora (Protector de pantalla o salvapantallas activo, Sesión de usuario bloqueada, Sesión de usuario finalizada) mm. La solución deberá contar con un módulo de protección contra Botnets, este módulo debe ser capaz de detectar conexiones con servidores maliciosos. nn. Firewall personal, la solución de antivirus debe contar con un firewall personal y debe tener los siguientes modos de configuración: • Modo automático • Modo interactivo • Modo basado en políticas • Modo aprendizaje oo. Las reglas de firewall creadas deberán ser capaces de permitir todas las siguientes acciones: • Denegar • Permitir • Preguntar pp. La solución deberá integrar un navegador seguro (Chrome), mostrando el logotipo de la solución presentada para asegurar que el módulo funcione correctamente, dando seguridad para proteger las transacciones bancarias, pagos en línea y sitios web. qq. La solución presentada incluirá una protección con el teclado, contra registradores de pulsaciones.

	ESPECIFICACIONES TÉCNICAS DE LAS LICENCIAS DE SEGURIDAD AVANZADA ENDPOINT DETECTION & RESPONSE (EDR) a. La solución debe ofrecer detección y respuesta en tiempo real a eventos maliciosos que ocurren en puntos finales, incluidos scripts maliciosos, ejecución anormal, malware sin archivos (fileless), exploits de aplicaciones y sistemas operativos, actividades de proceso anormales, scrapes de memoria y credenciales, shells inversos que tomen acciones maliciosas, exploits de día cero, ataques solo de memoria. b. La solución debe detectar acciones maliciosas en un equipo mediante técnicas de comportamiento (no basadas en firmas), y algoritmos de inteligencia artificial. c. La solución debe brindar protección contra ataques de día cero, mediante el análisis de comportamiento en el punto final, sin depender de firmas y reglas manuales. d. El agente debe incluir la creación de contexto de atributos en tiempo real de manera autónoma y automatizada, así como la correlación de eventos entre procesos (Storyline). e. La plataforma ofrecida debe unificar y ampliar la capacidad de detección y respuesta a través de múltiples capas de seguridad y debe incluir protección de endpoints (EPP), detección y respuesta de endpoints (EDR) en un solo agente para Windows, Mac, Linux, protección Kubernetes, S3, SDK y ambientes de almacenamiento como NETAPP f. La solución debe poder analizar eventos localmente en el agente sin dependencia de la nube. g. La solución no debe de tener dependencias de ciertos niveles de Kernel en Sistema Operativos de Linux. h. La solución no debe de depender de reinicio después de actualización del agente de protección o no debe de entrar en modo de protección reducida después de actualización de agente. i. La solución deberá soportar la instalación en Sistemas Operativos Windows Server 2003, 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, 2022 Y 2025 j. La solución ofrecida debe admitir cargas de trabajo de usuario final, en servidores y nativas de la nube. k. La solución ofrecida debe tener la capacidad de proteger Workloads k8 de usuario final, en servidores y nativas de la nube l. Automatización a nivel de protección y respuesta sin depender de los datos históricos; debe proteger durante todo el ciclo de vida de la amenaza (pre-ejecución, ejecución) m. Debe ser una solución de agente único, sin módulos adicionales, que se instalará en equipos, portátiles, servidores o máquinas virtuales, en sistemas operativos Windows, Linux y MacOS n. Detectar y contener la ejecución de malware avanzado, explotación de vulnerabilidades y malware de día 0 en el dispositivo final (PCs y Servidores). Debe ser basada en el análisis del comportamiento de la amenaza y su contexto en tiempo real sin el uso de reglas, firmas, conexión a la nube o sandbox. o. Debe tener la capacidad de remediar cambios al sistema operativo de manera automática usando la información aprendida por el agente de detección basado sobre el contexto de evolución de la amenaza para máquinas Windows y Mac p. Debe tener la capacidad de revertir cambios a archivos afectados durante un incidente en máquinas Windows (rollback) sin tener la necesidad de utilizar secuencia de comandos y debe ejecutarse manera automatizada, y/o con un solo con 1 solo click desde la consola en caso de ataques de ransomware. No debe de tener límite

	de numero de archivos o tamaño de archivos. Se debe de soportar archivos de 100 megas o más. q. La solución ofrecida debe permitir la conexión vía línea de comandos directamente desde la consola de administración a máquinas Windows, Mac, Linux y K8 con privilegios de sistema con una cuenta dinámica, que permita realizar investigación de ataques, recopilar datos forenses y remediar infracciones, sin importar dónde se encuentren los puntos finales comprometidos, eliminando la incertidumbre y reduciendo en gran medida cualquier tiempo de inactividad que resulte de un ataque. r. La solución ofrecida debe proveer una característica que permita aislar un punto final de la red, excepto de la consola de administración, con propósito preventivo para detener la propagación de un incidente mientras se investiga una alerta. El aislamiento debe de tener la capacidad de agregar diferentes políticas de acceso en el caso que se necesite conectar el equipo a otros recursos. s. La solución debe contar con la opción para limitar la cantidad de agentes que pueden descargar una actualización en un momento dado. t. La solución debe contar con la capacidad de heredar políticas en cualquier nivel, así como especificar la política por un sitio específico. u. La solución debe contar con la opción de "Dar de baja automáticamente" a los agentes antiguos si no se han comunicado con la consola de administración durante un período de tiempo configurable. v. La solución debe permitir la actualización de los agentes desde la consola de administración o mediante una carpeta compartida w. La solución ofrecida debe estar posicionada en el cuadrante de líderes de Gartner en los últimos tres años. x. La solución ofrecida debe participar en el análisis anual de MITRE ATT&CK para soluciones EDR y debe tener un cumplimiento mínimo del 99% en cada criterio de evaluación en los últimos 2 años y posicionada en el cuadrante mágico de gartner para soluciones EPP en la categoría de líderes o challenger. y. Debe permitir la detección, remediación y respuesta automatizada ante amenazas avanzadas, haciendo el mapeo de los indicadores de sistemas operativos Windows vigentes y Mac de amenazas con el framework de MITRE. z. Debe tener la capacidad de detección de amenazas avanzadas basado en Inteligencia artificial y por comportamiento localmente en el agente sin depender de reglas-preprogramadas. aa. Debe permitir la creación de reportes que se puedan exportar desde la consola de administración. bb. Debe permitir la visualización de todos los procesos/eventos que genera la detección. cc. Debe contar con las funcionalidades de control de dispositivos (USB, Bluetooth y thunderbolt) dd. Debe contar con la funcionalidad de control de firewall local. ee. La solución debe brindar visibilidad de aplicaciones instaladas en los dispositivos finales indicando su nivel de riesgo, inventario de aplicaciones y vulnerabilidades asociadas ff. La plataforma debe unificar las funciones de prevención y detección de dispositivos, detección de puntos finales y rendición de cuentas sin depender de datos históricos, y debe realizar funciones de detección y ejecución automáticas, búsqueda de incidentes de seguridad en una única solución. gg. Los agentes de la solución ofrecida deben ser resistentes a la manipulación y tener una lógica local de prevención, detección y

	respuesta para que el propio agente reduzca significativamente la duración de la permanencia del ataque. hh. Debe guardar 365 días de historial de datos de incidentes almacenados directamente en la consola. ii. II. El agente debe ser autónomo, realizar detección y mitigación en tiempo real sin la ayuda o intervención de un Centro de Operaciones de Seguridad (SOC). jj. La solución debe clasificarse como ACTIVE EDR – XDR. kk. Debe ser una consola multiusuario, multisitio y multigrupo que permita la creación de usuarios con independencia y accesos con diferentes roles. ll. La consola de administración debe implementar la API RESTFUL o equivalente para fines de integración con herramientas de cualquier sistema que admita la integración de API. mm. La autenticación en la plataforma puede realizarse haciendo SSO y habilitando un segundo factor de autenticación para validar otro parámetro y confirmar la petición del usuario. nn. La solución debe controlar los "grupos dinámicos" en función de etiquetas (TAGS) u otros atributos. Asegurando de que esté disponible en todas las superficies, incluidas: Windows, macOS, Linux, K8s, etc oo. Debe incluir un catálogo de exclusiones (mínimo 78 aplicaciones) para los procesos corriendo en los sistemas operativos en Windows, macOS, Linux y contenedores. pp. La auditoría y el registro de actividad deben mantenerse en la consola de administración. qq. La solución a ofertar debe tener una base de conocimiento y documentación dentro de la consola sin la necesidad de utilizar credenciales de otro sistema. rr. La solución debe tener una plataforma avanzada que centralice datos de tu entorno y de seguridad, facilitando la detección temprana y la respuesta rápida a amenazas al consolidar datos EDR, XDR y de terceros en una sola consola unificada. ss. La solución debe permitir hacer integraciones con soluciones de seguridad de terceros a través de su Marketplace que sea simple de configurar y administrar. tt. Debe permitir integraciones XDR de tipo "Automatizacion" y "Enriquecimiento" con aplicaciones via un Marketplace API con aplicaciones como Okta. uu. La solución debe permitir la configuración en modo de detección o protección en sistemas operativos Linux. vv. El producto admite cargas de trabajo (Cloud Workloads) en la nube que se ejecutan en Azure, AWS o Google Cloud. ww. Extensión de Azure disponible para facilitar la implementación dentro de Azure. xx. La solución debe permitir el acceso vía API completo a todas las capacidades de gestión y acceso a los datos. yy. La auditoría y el registro de actividad deben mantenerse en la consola de administración. La solución debe contar con la capacidad de enviar registros a una fuente externa (SIEM, etc.). zz. Los datos deben estar cifrados tanto en el almacenamiento como en reposo. aaa. La solución debe brindar capacidades de EPP y EDR disponibles en un solo agente sin necesidad de instalar varios paquetes de software. bbb. La solución debe contar con Anti-tamper. ccc. Capacidad para iniciar análisis bajo demanda para buscar malware o asegurarse de que se haya corregido una amenaza (desde la consola y / o el punto final).

	ddd. Capacidad para programar actualizaciones de agentes desde la consola de administración. eee. La solución debe contar con la opción para limitar la cantidad de agentes que pueden descargar una actualización en un momento dado. fff. El producto no debe dejar de funcionar si se excede la cantidad de licencias adquiridas. ggg. La solución debe contar con la opción de "Dar de baja automáticamente" a los agentes antiguos si no se han comunicado con la consola de administración durante un período de tiempo configurable. hhh. El agente debe tener un rendimiento mínimo del sistema bajo carga estándar (1-2% de CPU, <250 Mb de memoria). iii. La solución debe permitir realizar acciones de respuesta XDR la cual podrá detener la expansión del ataque.
	CONSOLA DE ADMINISTRACIÓN CENTRALIZADA - La consola debe ser con infraestructura en la nube, implementado como un servicio SAAS, no debe ser necesario de un servidor local para su implementación. - La consola de administración debe permitir la configuración y administración remota de la solución antivirus instalada en las estaciones de trabajo y servidores (Windows, Linux, Mac). Soporte para dispositivos móviles. - Debe permitir la delegación de tareas mediante creación de usuarios con distintos perfiles de administración, de tal manera que se puedan agregar usuarios con diferentes niveles de acceso o permisos. - Por medidas de seguridad la consola de administración debe contar con un doble factor de autenticación para ingresar a la consola, que consiste en una contraseña permanente y una contraseña adicional o token de un solo uso. - La consola debe tener medidas de protección de acceso frente a ataques de fuerza bruta, como bloquear el acceso luego de varios intentos fallidos de inicio de sesión. - La consola de acceso al servidor deberá ser 100% web, siendo compatible con los siguientes navegadores: Mozilla Firefox, Microsoft SCCM, Google Chrome, Safari, Opera. - El servidor se deberá comunicar con los endpoints a través de un agente que sea capaz de almacenar las políticas y ejecutar tareas de manera offline. - El acceso a la consola a través del interfaz web se bloqueará de forma temporal (aproximadamente 10 minutos), luego de 10 intentos de inicio de sesión no satisfactorios, desde una misma dirección IP. - El producto debe ser capaz de mostrar los equipos detectados en la red. - La consola de administración centralizada debe tener la capacidad de mostrar los intentos de infección de virus en los equipos clientes. - El producto debe ser capaz de controlar a través de políticas todos los componentes mencionados anteriormente (para Workstation y servers) sin necesidad de consolas adicionales para la creación de políticas. - El producto debe poseer una interfaz web que permita monitorear el estado de los equipos en la red, así como también, mostrar como mínimo reportes sobre: el estado de carga del servidor, clientes con mayor registro de amenazas, principales amenazas, clientes con más amenazas, clientes actualizados /no actualizados y sistemas operativos administrados.

	- El producto debe permitir la instalación y desinstalación remota de los servidores y clientes antivirus. - El producto debe ser capaz de crear tareas de desinstalación del propio antivirus y de antivirus de terceros. - El producto debe permitir la generación de reportes gráficos y personalización de estos. - Los reportes deben ser fácilmente exportables en formatos CSV, PDF. - El producto debe ser capaz de escanear la red por Directorio Activo, Red IP o Dominios, o una tecnología propia de detección de equipos; en busca de nuevos equipos agregados a la red. - El producto debe ser capaz de generación de alertas ante un evento específico mediante el envío de un correo. - Las actualizaciones deben ser descargadas directamente desde los servidores del fabricante y con la opción de usar para que los clientes actualicen desde el servidor de administración sus definiciones de virus, phishing, spam, bases de datos de URLs maliciosas, actualización de parches del producto entre otras. - Debe permitir gestionar licencias, ya sea como propietario de estas o como administrador de seguridad. Puede llevar un seguimiento de las licencias y los equipos activados con esta, además de observar sucesos relacionados con las licencias como son la caducidad, el uso y las autorizaciones. Esto sin necesidad de consultar la consola de administración. - La solución debe permitir el manejo flexible de las licencias, de manera que puedan ser reasignadas en caso se restaure el sistema o se cambie de equipo. - Deberá permitir la ejecución remota de scripts, batch files y paquetes personalizados de terceros a través de la consola. - Deberá permitir generar grupos de clientes dinámicos y grupos estáticos. **OTROS.** • El fabricante deberá tener soporte técnico en español y laboratorio de análisis de malware en Sudamérica para atender incidencias que afecten la región. • El fabricante deberá ocupar una posición de Leader o Challenger en el Cuadrante Mágico de Gartner del último año de publicación. • El Proveedor debe ser Partner registrado por la marca, el cual se acreditará mediante una carta. • El proveedor deberá adjuntar acreditar los certificados de las licencias adquiridas a nombre de la UGEL Cusco por el periodo de 1 año. • El proveedor deberá proporcionar asistencia técnica y soporte durante la vigencia de las licencias, incluyendo actualizaciones automáticas de definiciones de amenazas y mantenimiento de la plataforma de administración centralizada, a fin de asegurar la protección continua y la gestión integral de los equipos de cómputo y servidores institucionales.
6. REQUISITOS DEL CONTRATISTA	El contratista debe de cumplir con el siguiente perfil: ✔ Tener como actividad económica relacionada al objeto de la contratación. ✔ Estar Activo y habido en la SUNAT. ✔ Contar con inscripción vigente en el RNP, (en caso mayores de 1 UIT).

	✔ No tener impedimentos para contratar con el estado.
7. PLAZO DE ENTREGA	**PLAZO**: El plazo de entrega del bien será de 10 días calendarios, a partir del día siguiente de la notificación de la Orden de Compra.
8. LUGAR DE ENTREGA	**LUGAR:** El bien será entregado en el almacén central de la Unidad de Gestión Educativa Local del Cusco, ubicada en AV. Camino Real N° 114 Wánchaq – Cusco. **HORARIO DE ATENCION:** De 08:30 am a 13:00 pm de lunes a viernes De 14:00 pm a 16:30 pm de lunes a viernes
9. FORMA Y CONDICIONES DE PAGO	El pago se realiza de conformidad con lo establecido en el artículo 67 de la Ley. La entidad paga las contraprestaciones pactadas a favor del contratista dentro de los diez (10) días hábiles siguientes de otorgada la conformidad por parte del área usuaria y es prorrogable, previa justificación de la demora, por cinco días hábiles. El pago se realizará en un Único Pago al finalizar la entrega del bien. Previa firma de acta de conformidad del área usuaria. Para la procedencia de pago, el contratista deberá presentar la siguiente documentación: • Comprobante de pago • Copia de la Orden de Compra • Guía de remisión • Carta de autorización para pagos a Cuenta Interbancaria – CCI En caso de retraso en el pago por parte de la entidad, salvo que se deba acaso fortuito o fuerza mayor, EL CONTRATISTA tiene derecho al pago de intereses legales conforme a lo establecido en el artículo 67 de la Ley N° 32069, Ley General de Contrataciones Públicas Los pagos se realizarán como máximo a los 10 días calendarios de emitido la conformidad.
10. GARANTIAS	Según el Art.61 de la LGCP, el cumplimiento de las obligaciones de los contratistas debe ser garantizado a través de los mecanismos establecidos en la presente ley, a fin de cubrir el adelanto de pago, y el fiel cumplimiento del contrato, así como el fiel cumpliendo de las prestaciones accesorias.

11. CONFORMIDAD DEL BIEN	La conformidad de la prestación del servicio se regula por lo dispuesto en el artículo 144 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado mediante Decreto Supremo N° 009-2025. LA CONFORMIDAD ES OTORGADA POR RESPONSABLE DE LA OFICINA DE INFORMATICA DE LA UGEL CUSCO el plazo máximo de SIETE (7) DÍAS MÁXIMO, días computados desde el día siguiente de recibido el entregable o servicio. De existir observaciones, la Entidad las comunica al CONTRATISTA, indicando claramente el sentido de estas, otorgándole un plazo para subsanar dependiendo de la complejidad o sofisticación de las subsanaciones a realizar. El plazo de subsanación no debe ser mayor del 30% del plazo del entregable correspondiente. Si pese al plazo otorgado, EL CONTRATISTA no cumpliese a cabalidad con la subsanación, la Entidad puede otorgar al CONTRATISTA periodos adicionales para las correcciones pertinentes. En este supuesto corresponde aplicar la penalidad por mora desde el vencimiento del plazo para subsanar sin considerar los días en los que pudiera incurrir la Entidad para efectuar las revisiones y notificar las observaciones correspondientes. Este procedimiento no resulta aplicable cuando los servicios manifiestamente no cumplan con las características y condiciones ofrecidas, en cuyo caso la entidad no efectúa la recepción o no otorga la conformidad, según corresponda, debiendo considerarse como no ejecutada la prestación, aplicándose la penalidad que corresponda por cada día de atraso.
12. PENALIDAD	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 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: Penalidad diaria = 0.10 X monto F X plazo en días Donde F tiene los siguientes valores: F = 0.40 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. El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobado. Adicionalmente, se considera justificado el retraso y en consecuencia no se aplica penalidad, cuando EL CONTRATISTA acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En este último caso la calificación del retraso como justificado por parte de la entidad no da lugar al pago de gastos generales ni costos directos de ningún tipo, conforme al numeral 120.4 del artículo 120 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF. Las penalidades se deducen de los pagos a cuenta, pagos parciales o del pago final, según corresponda.
13. RESOLUCION DE CONTRATO POR INCUMPLIMIENTO	Cualquiera de las partes puede resolver el contrato, de conformidad con el numeral 68.1 del artículo 68 de la Ley N° 32069, Ley General de Contrataciones Públicas. De encontrarse en alguno de los supuestos: 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 prestación 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.
14. GESTION DE RIESGOS	Las partes realizan la gestión de riesgos de acuerdo con lo establecido en el presente documento, a fin de tomar decisiones informadas, aprovechando el impacto de riesgos positivos y disminuyendo la probabilidad de los riesgos negativos y su impacto durante la ejecución contractual, considerando la finalidad pública de la contratación.
15. CLAUSULA SOLUCION DE CONTROVERSIAS	Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación o arbitraje, según el acuerdo de las partes. Cualquiera de las partes tiene derecho a iniciar el arbitraje a fin de resolver dichas controversias dentro del plazo de caducidad

	El Laudo arbitral emitido es inapelable, definitivo y obligatorio para las partes desde el momento de su notificación, según lo previsto en el numeral 84.9 del artículo 84 de la Ley N° 32069, Ley General de Contrataciones Públicas.
16. CLAUSULA ANTCORRUPCION Y ANTISOBORNO	A la suscripción de este contrato, 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. 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, 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. 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 del presente contrato. Finalmente, el incumplimiento de las obligaciones establecidas en esta cláusula, durante la ejecución contractual, otorga a la entidad 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.

GOBIERNO REGIONAL CUSCO
GERENCIA REGIONAL EDUCACION CUSCO
UNIDAD DE GESTION EDUCATIVA LOCAL CUSCO
Ing. Yolvi Quispe Rocca
JEFE DE EQUIPO DE INFORMATICA

ANEXO N°01:
DECLARACIÓN JURADA DEL PROVEEDOR

"DE NO ESTAR IMPEDIDO PARA CONTRATAR CON EL ESTADO Y DE CUMPLIMIENTO DE REQUERIMIENTOS TÉCNICOS MÍNIMOS"

Señor:
Dr. Freddy Quiñones Cárdenas.
Director de la UGEL- Cusco

Presente.-

Mediante el presente el suscrito, postor y/o Representante Legal de ..... con RUC N°: ..... declaro bajo juramento:

1. **No tener impedimento para contratar con el Estado,** conforme al artículo 30° de la Ley N° 32069, Ley General de Contrataciones Públicas.
2. Ser responsable de la veracidad y autenticidad de los documentos e información que presento.
3. Conocer, aceptar y someterme a las condiciones y procedimientos de la presente contratación.
4. Comprometerme a mantener la oferta (precio, condiciones y obligaciones) presentadas en mi cotización y de cumplir con la Orden de Compra / Servicio, en caso de ser favorecido con la contratación.
5. Conocer las sanciones contenidas en la Ley General de Contrataciones Públicas y su Reglamento, la Ley N° 27444, Ley del Procedimiento Administrativo General y la Ley N° 27815, Ley del Código de Ética de la Función Pública.
6. Actuaré conforme a los principios previstos en la Ley General de Contrataciones Públicas

Cusco, de del 202

.....
Firma, Nombres y Apellidos de/ proveedor o Representante legal, según corresponda

*DNI N° :*_____

*RUC N:*_____

ANEXO N°02:
DECLARACIÓN JURADA DEL PROVEEDOR

Señores: **UNIDAD DE GESTIÓN EDUCATIVA LOCAL - CUSCO**

El que se suscribe, identificado con Documento Nacional de Identidad N°.....representante legal de la empresa:

Nombre o Razón Social:		
Domicilio Legal:		
RUC:	Teléfono:	Teléfono Celular:
Correo Electrónico:		
Persona de Contrato:		N° DNI:

DECLARO BAJO JURAMENTO, que la siguiente información se sujeta a la verdad:

1. No tiene impedimento ni está inhabilitado para contratar con el Estado.
2. Es responsable de la veracidad de los documentos e información que presenta a efectos del presente proceso de contratación
3. Conoce las sanciones contenidas en la Ley N° 27444, Ley del Procedimiento Administrativo General.
4. Conoce y acepta las modalidades de comunicación señaladas en el numeral 20.1.2 del artículo 20 de la Ley 27444, Ley del Procedimiento Administrativo General.
5. Sus representantes legales no tienen grado de parentesco hasta el 4 grado de consanguinidad o 2° de afinidad, ni por razón de matrimonio o por unión de hecho, con tos funcionarlos o servidores de la UNIDAD DE GESTION EDUCATIVA LOCAL — CUSCO.
6. Su cuenta Interbancaria (CCI).

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

NOMBRE DEL BANCO:

por lo que los pagos a su nombre deben ser abonados en la cuenta que corresponde al Indicado CCI en el Banco Indicado.

7. Cuenta con inscripción vigente y habido en el Registro Único del Contribuyente (RUC)
8. Cuenta con Inscripción vigente en el Registro Nacional de Proveedores (RNP) en el rubro del objeto de la contratación (En caso el importe de la cotización sea igual o mayor a 1 UIT).
9. El correo electrónico es el medio oficial, donde se notificará ampliación de plazo resolución de contrato u orden de compra y servicio. Siendo contabilizado al día siguiente de su recepción.
10. Declara y garantiza no haber. Directo o indirectamente, o tratándose de una persona natural o jurídica a través de sus socios, integrantes de los órganos de administración. Apoderados, representantes legales funcionarios asesores o personas vinculadas.
11. Asimismo, se obliga a conducirse en todo momento, durante la ejecución del contrato u orden de compra y servicio, con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participacioncitas, integrantes de los órganos de administración, apoderados, representantes legales funcionarios, asesores y personas vinculadas.

Cusco, de del 202

.....
Firma, Nombres y Apellidos del Proveedor
O Representante Legal, según corresponda

ANEXO N° 03
DECLARACION JURADA ANTISOBORNO

Yo, ...(Representante Legal de .....),con Documento de Identidad N°.....en representación de....., en adelante EL CONTRATISTA con RUC N°..... declaro lo siguiente:

EL CONTRATISTA no ha ofrecido, negociado o efectuado, cualquier pago, objeto de valor o cualquier dádiva en general, o cualquier beneficio o incentivo ilegal en relación al contrato, que pueda constituir un incumplimiento a la Ley, tales como robo, fraude, cohecho o tráfico de influencias, directa o indirectamente, o a través de socios, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios , asesores o personas vinculadas, en concordancia a lo establecido en la Ley N°32069, Ley General de Contrataciones Públicas y su Reglamento.

Asimismo, **EL CONTRATISTA** se obliga a conducirse en todo momento, durante la ejecución del contrato, con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participantes, integrantes de los órganos de administración apoderados, representantes legales, funcionarios, asesores y personas vinculadas en virtud a lo establecido en concordancia o a lo establecido en la Ley N°32069, Ley General de Contrataciones Públicas y su Reglamento.

Asimismo, **EL CONTRATISTA** se compromete a comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; así también en adoptar medidas técnicas, prácticas, a través de los canales dispuestos por la entidad.

De la misma manera, **EL CONTRATISTA** es consciente que, de no cumplir con lo anteriormente expuesto, se someterá a la resolución del contrato y a las acciones civiles y/o penales que la entidad pueda accionar.

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. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar

Cusco, ... de.....Del 202

.....

Nombre, firma y sello del solicitante o Rep. Legal de la empresa