SOLICITUD DE COTIZACIÓN

UNIDAD EJECUTORA : 312 GOB. REG. DPTO. CUSCO - UGEL CUSCO
NRO. IDENTIFICACIÓN : 001644

Señores	:			R.U.C.	
Dirección	:				
Teléfono	:		Fax :		
Nro. Cons.	: 136	Fecha : 25/09/2023		Documento :	
Concepto	:				

CANTIDAD REQUERIDA	UNIDAD MEDIDA	DESCRIPCION	PRECIO UNITARIO	PRECIO TOTAL
114.00	UNIDAD	SOFTWARE ANTIVIRUS TÉRMINO DE REFERENCIA: ESPECIFICACIONES TECNICAS ESPECIFICACIONES TECNICAS DEL ANTIVIRUS SOLUCIÓN DE PROTECCIÓN PARA ESTACIONES DE TRABAJO. 1.La solución y/o producto ofertado (en sus últimas versiónes) deberá ser compatible con los siguientes sistemas operativos: Microsoft® Windows® 11/10/8.1/8/7. 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, CentOS y superior. 2.La solución y/o 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. 3.La solución y/o 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. 4.La solución y/o 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 5.La solución y/o producto ofertado debe ser capaz de detectar todo tipo de amena zas, entre los más comunes: virus, gusanos, troyanos, spyware, adware, rootkits, bots, ransomware, etc. 6.La solución y/o producto ofertado deberá contar con una funcionalidad antiransomware. 7.La solución y/o 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. 8.La solución y/o producto ofertado 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		

SOLICITUD DE COTIZACIÓN

UNIDAD EJECUTORA : 312 GOB. REG. DPTO. CUSCO - UGEL CUSCO
NRO. IDENTIFICACIÓN : 001644

Señores :
Dirección :
Teléfono :
Nro. Cons. : 136
Concepto :

R.U.C.

Fax :
Fecha : 25/09/2023
Documento :

CANTIDAD REQUERIDA	UNIDAD MEDIDA	DESCRIPCION	PRECIO UNITARIO	PRECIO TOTAL
		TÉRMINO DE REFERENCIA: configurar para realizarse una vez o repetirse a diferentes intervalos, días, semanas, meses, etc. 9.La solución y/o producto ofertado debe permitir elegir las unidades a escanear para los escaneos bajo demanda. 10.La solución y/o producto ofertado debe ser capaz de crear exclusiones de escaneo ya sea por archivo, extensión o carpeta específica. 11.La solución y/o producto ofertado debe pedir una contraseña ante intentos de cambio indebidos en la configuración del producto. 12.La solución y/o producto ofertado 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. 13.La solución y/o 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. 14.La solución y/o 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. 15.La solución y/o 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. 16.La solución y/o producto ofertado debe tener sistema de prevención de intrusiones basado en el host, (HIPS). 17.El sistema HIPS de la solución y/o producto ofertado debe tener los siguientes modos de configuración: automático, inteligente, interactivo,		

SOLICITUD DE COTIZACIÓN

UNIDAD EJECUTORA : 312 GOB. REG. DPTO. CUSCO - UGEL CUSCO
NRO. IDENTIFICACIÓN : 001644

Señores	:			R.U.C.
Dirección	:			
Teléfono	:	Fax	:	
Nro. Cons.	: 136	Fecha : 25/09/2023	Documento :	
Concepto	:			

CANTIDAD REQUERIDA	UNIDAD MEDIDA	DESCRIPCION	PRECIO UNITARIO	PRECIO TOTAL
		TÉRMINO DE REFERENCIA: basado en políticas y aprendizaje. 18.La solución y/o producto ofertado debe poseer un firewall bidireccional que posea minimo 4 modos de filtrado entre ellos, automático, interactivo, aprendizaje y modo basado en políticas, además que pueda tener la capacidad de bloquear conexiones entrantes y salientes. 19.La solución y/o producto ofertado debe tener la capacidad de tener un filtro web con un minimo de 27 categorías entre las cuales se deba permitir o bloquear el acceso a las webs según el administrador lo disponga. 20.La solución y/o producto ofertado permitirá crear grupos que contengan varios vínculos URL para crear reglas de permiso y bloqueo a determinados sitios web. 21.El bloqueo web de la solución y/o producto ofertado deberá poder asignarse por un rango de tiempo, por grupo y por equipo. 22.La solución y/o producto ofertado debe tener un filtro antispam que permita integrarse con clientes como Microsoft Outlook. Esta funcionalidad debe permitir al usuario crear una lista negra o blanca de direcciones de correo. 23.La solución y/o producto ofertado deberá analizar protocolos de e-mail POP3, IMAP, MAPI. 24.La protección del correo electrónico en el cliente de la solución y/o producto ofertado debe permitir definir si se desea escanear sólo correo recibido, correo enviado o correo leido. 25.La solución y/o producto ofertado debe tener la capacidad de añadir una nota o etiqueta en los correos electrónicos recibidos o leidos. 26.La solución y/o producto ofertado 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. 27.La solución y/o producto ofertado debe tener un módulo de protección en tiempo real para		

SOLICITUD DE COTIZACIÓN

UNIDAD EJECUTORA : 312 GOB. REG. DPTO. CUSCO - UGEL CUSCO
NRO. IDENTIFICACIÓN : 001644

Señores :
Dirección :
Teléfono :
Fax :
Nro. Cons. : 136
Fecha : 25/09/2023
Documento :
Concepto :
R.U.C.

CANTIDAD REQUERIDA	UNIDAD MEDIDA	DESCRIPCION	PRECIO UNITARIO	PRECIO TOTAL
		TÉRMINO DE REFERENCIA: el acceso a la web. 28.La solución y/o producto ofertado debe ser capaz de escanear a través del protocolo SSL (HTTPS), de manera que se pueda impedir la descarga de archivos infectados. 29.La solución y/o producto ofertado debe de permitir realizar exclusiones de URL para que no sean analizadas por el antivirus tanto en el protocolo HTTP, y HTTPS. 30.La solución y/o 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. 31.La solución y/o 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). 32.La solución y/o producto ofertado debe ser capaz de crear CD's, ISO's o USB de rescate, que permitan escanear los equipos Microsoft. 33.La solución y/o producto ofertado 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. 34.La solución y/o producto ofertado 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. 35.La solución y/o producto ofertado debe contar con una herramienta que permita examinar a fondo el ordenador,		

SOLICITUD DE COTIZACIÓN

UNIDAD EJECUTORA : 312 GOB. REG. DPTO. CUSCO- UGEL CUSCO
NRO. IDENTIFICACIÓN : 001644

Señores : **R.U.C.**
Dirección :
Teléfono : **Fax** :
Nro. Cons. : 136 **Fecha** : 25/09/2023 **Documento** :
Concepto :

CANTIDAD REQUERIDA	UNIDAD MEDIDA	DESCRIPCION	PRECIO UNITARIO	PRECIO TOTAL
		TÉRMINO DE REFERENCIA: 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). 36.La solución y/o producto ofertado deberá poder realizar exploraciones en estado inactivo para poder brindar de esa forma, una protección proactiva mientras el equipo no está en uso. 37.La solución y/o producto ofertado debe contar con la funcionalidad de bloqueo de exploits, que evite la explotación de vulnerabilidades en las aplicaciones. 38.La solución y/o producto ofertado debe contar con un modo transparente de uso, en el cual no muestre ninguna alerta cuando se esté ejecutando una aplicación en pantalla completa. 39.La solución y/o producto ofertado 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. 40.La solución y/o producto ofertado 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) 41.La solución y/o producto ofertado deberá contar con un módulo de protección contra Botnets, este módulo debe ser capaz de detectar conexiones con servidores maliciosos. 42.La solución y/o producto ofertado 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		

SOLICITUD DE COTIZACIÓN

UNIDAD EJECUTORA : 312 GOB. REG. DPTO. CUSCO - UGEL CUSCO
NRO. IDENTIFICACIÓN : 001644

Señores :
R.U.C.
Dirección :
Teléfono : **Fax** :
Nro. Cons. : 136 **Fecha** : 25/09/2023 **Documento** :
Concepto :

CANTIDAD REQUERIDA	UNIDAD MEDIDA	DESCRIPCION	PRECIO UNITARIO	PRECIO TOTAL
		TÉRMINO DE REFERENCIA: transacciones bancarias, pagos en linea y sitios web. 43.La solución y/o producto ofertado incluirá una protección con el teclado, contra registradores de pulsaciones. A.SOLUCIÓN DE PROTECCIÓN PARA SERVIDORES Se debe considerar La solución y/o producto ofertado (en sus últimas versiónes), para todos los servidores, con las siguientes caracteristicas: 1.La solución y/o producto ofertado debe poder instalarse en su última versión, sobre plataformas Windows 2008 Server R2 SP1, small business server 2011(x64), Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022 y Server Core (Windows Server 2008 R2 SP1 Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 y Windows Server 2022) 2.La solución y/o producto ofertado debe poder instalarse sobre plataformas de x64 bits RedHat Enterprise Linux (RHEL) 7 y 8; CentOS 7 y 8; Ubuntu Server 16.04, 18.04 y 20.04 LTS; Debian10 y 11; SUSE Linux Enterprise Server (SLES) 12 y 15. 3.La solución y/o producto ofertado debe ser compatible con versiones del kernel del sistema operativo Linux 3.10.0 y posteriores 4.La solución y/o producto ofertado debe contar con un módulo de detección en tiempo real que proteja contra códigos maliciosos en cada acción realizada en el equipo (abrir, crear o ejecutar) 5.La solución y/o producto ofertado debe ser capaz de detectar todo tipo de amenazas, entre los más comunes: virus, gusanos, troyanos, spyware, adware, rootkits, bots, ransomware, etc. 6.La solución y/o producto ofertado deberá contar con una funcionalidad antiransomware. 7.La solución y/o producto ofertado debe ser capaz de evitar que sus procesos, servicios, archivos o archivos de registro puedan ser detenidos, deshabilitados,		

SOLICITUD DE COTIZACIÓN

UNIDAD EJECUTORA : 312 GOB. REG. DPTO. CUSCO - UGEL CUSCO
NRO. IDENTIFICACIÓN : 001644

Señores :
Dirección :
Teléfono :
Fax :
Nro. Cons. : 136
Fecha : 25/09/2023
Documento :
Concepto :
R.U.C.

CANTIDAD REQUERIDA	UNIDAD MEDIDA	DESCRIPCION	PRECIO UNITARIO	PRECIO TOTAL
		TÉRMINO DE REFERENCIA: eliminados o modificados, para de esta manera garantizar su funcionamiento ante cualquier tipo de ataque de virus. 8.La solución y/o producto ofertado para servidores Windows deberá contar con exclusiones automáticas que permitan detectar las aplicaciones críticas del servidor y los archivos críticos del sistema operativo y los agregue automáticamente a la sección de exclusiones al momento de ser instalado. 9.La solución y/o producto ofertado debe ser capaz de crear exclusiones de escaneo ya sea por archivo, extensión o carpeta especifica. 10.La solución y/o producto ofertado debe pedir una contraseña ante intentos de cambio indebidos en la configuración del producto. 11.La solución y/o producto ofertado 11.La solución y/o producto ofertado debe contar con un agente que le permita ser administrado desde una consola centralizada. 12.La solución y/o producto ofertado debe permitir generar dentro de la misma solución antivirus repositorios de actualización, los cuales deberán ser distribuidas mediante protocolo http localmente, esto sin depender de aplicacio localmente, esto sin depender de aplicaciones externas o de la consola de Administración. 13.La protección en tiempo real de la solución y/o producto ofertado debe iniciarse con el sistema operativo, así como poder definir qué tipos de medios serán analizados por el módulo. 14.La solución y/o producto ofertado debe tener sistema de prevención de intrusiones basado en el host, (HIPS). 15.El sistema HIPS de la solución y/o producto ofertado debe tener los siguientes modos de configuración: automático, inteligente, interactivo, basado en políticas y aprendizaje. 16.La solución y/o producto ofertado debe permitir escanear archivos comprimidos. 17.La solución y/o producto ofertado debe permitir		

SOLICITUD DE COTIZACIÓN

UNIDAD EJECUTORA : 312 GOB. REG. DPTO. CUSCO - UGEL CUSCO
NRO. IDENTIFICACIÓN : 001644

Señores	:			R.U.C.	
Dirección	:				
Teléfono	:		Fax :		
Nro. Cons.	: 136	Fecha : 25/09/2023		Documento :	
Concepto	:				

CANTIDAD REQUERIDA	UNIDAD MEDIDA	DESCRIPCION	PRECIO UNITARIO	PRECIO TOTAL
		TÉRMINO DE REFERENCIA: elegir las unidades a escanear para los escaneos bajo demanda. 18.En sistemas operativos Windows, la solución y/o producto ofertado deberá contar con una herramienta integrada que permita inspeccionar completamente componentes del sistema (Controladores, Aplicaciones Instaladas, Conexiones de Red y entradas importantes del Registro de Windows), esto con la finalidad de determinar la causa de comportamientos sospechosos en el sistema que puede deberse a incompatibilidad de software, hardware o código malicioso. 19.La solución y/o producto ofertado debe tener un caché local para aumentar el rendimiento de los entornos virtuales, garantizando que el archivo sólo se explora una vez. B.SANDBOXING. 1.Uso de Sandboxing en la nube para analizar el comportamiento de archivos, con SLA de 5 minutos hasta 1 hora de respuesta. 2.Es posible crear una exclusión por ruta, detección y su hash (SHA-1) 3.Capacidad de sincronizar su licenciamiento con la nube y la consola de administración en sitio o en la nube. 4.Detectar un archivo sospechoso ejecutado por primera vez se debe mostrar una advertencia, si el análisis se completa antes de ejecutar el archivo por primera vez, no se muestra el aviso archivo en análisis. 5.Debe borrar automáticamente las muestras de los archivos/ejecutables en los servidores donde fue analizado el comportamiento. 6.Capacidad para enviar correos SPAM para su análisis. 7.Debe tener únicamente estos umbrales de detección: desconocido, limpio, sospechoso, altamente sospechoso y malicioso. 8.Debe tener la siguiente información de un archivo enviado al Sanboxing en la nube: nombre del equipo desde donde se ingresó el archivo, el usuario que lo ingresó, la razón, hash en SHA-1,nombre del archivo ingresado, tamaño del archivo, categor		

SOLICITUD DE COTIZACIÓN

UNIDAD EJECUTORA : 312 GOB. REG. DPTO. CUSCO - UGEL CUSCO
NRO. IDENTIFICACIÓN : 001644

Señores :
Dirección :
Teléfono :
Fax :
R.U.C.
Nro. Cons. : 136
Fecha : 25/09/2023
Documento :
Concepto :

CANTIDAD REQUERIDA	UNIDAD MEDIDA	DESCRIPCION	PRECIO UNITARIO	PRECIO TOTAL
		TÉRMINO DE REFERENCIA: 9.Debe tener protección proactiva, es decir, que el archivo/ejecutable sea bloqueado hasta recibir el resultado del Sandbox en la nube. 10.Se debe tener capacidad para integrarse con la solución de antivirus o protección del punto final, para tener mayores posibilidades de protección y aplicación de políticas. 11.Enviar un archivo/ejecutable a través de una consola de administración del punto final. C.CIFRADO DE DISCO. 1.La solución y/o producto ofertado deberá ser capaz de cifrar los Endpoints deseados desde el inicio de sistema. 2.La solución y/o producto ofertado deberá disponer de diversas posibilidades de recuperación de Passwords para usuarios remotos que se vean bloqueados. 3.La solución y/o producto ofertado deberá poder programar las tareas de cifrado sobre los Endpoints deseados con la posibilidad de pausar la ejecución para retomar luego desde el último punto. 4.La solución y/o producto ofertado deberá poder ser administrada desde la misma consola central junto con las otras soluciones descriptas en el TDR. D.CONSOLA DE ADMINISTRACIÓN CENTRALIZADA DE LA SOLUCIÓN Y/O PRODUCTO OFERTADO 1.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. 2.La consola de administración debe permitir la configuración y administración remota de la solución y/o producto ofertado, instalada en las estaciones de trabajo y servidores (Windows, Linux, Mac). Soporte para dispositivos móviles. 3.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. 4.Por medidas de seguridad		

SOLICITUD DE COTIZACIÓN

UNIDAD EJECUTORA : 312 GOB. REG. DPTO. CUSCO - UGEL CUSCO
NRO. IDENTIFICACIÓN : 001644

Señores :
Dirección :
Teléfono :
Fax :
R.U.C.
Nro. Cons. : 136
Fecha : 25/09/2023
Documento :
Concepto :

CANTIDAD REQUERIDA	UNIDAD MEDIDA	DESCRIPCION	PRECIO UNITARIO	PRECIO TOTAL
		TÉRMINO DE REFERENCIA: 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. 5.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. 6.La consola de acceso al servidor deberá ser 100% web, siendo compatible con los siguientes navegadores: Mozilla Firefox, Microsoft SCCM, Google Chrome, Safari, Opera. 7.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. 8.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. 9.El producto debe ser capaz de mostrar los equipos detectados en la red. 10.La consola de administración centralizada debe tener la capacidad de mostrar los intentos de infección de virus en los equipos clientes. 11.La solución y/o producto ofertado 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. 12.La solución y/o producto ofertado 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. 13.La solución y/o producto ofertado debe permitir la		

SOLICITUD DE COTIZACIÓN

UNIDAD EJECUTORA : 312 GOB. REG. DPTO. CUSCO - UGEL CUSCO
NRO. IDENTIFICACIÓN : 001644

Señores :
R.U.C.
Dirección :
Teléfono : **Fax** :
Nro. Cons. : 136 **Fecha** : 25/09/2023 **Documento** :
Concepto :

CANTIDAD REQUERIDA	UNIDAD MEDIDA	DESCRIPCION	PRECIO UNITARIO	PRECIO TOTAL
		TÉRMINO DE REFERENCIA: instalación y desinstalación remota de los servidores y clientes antivirus. 14.La solución y/o producto ofertado debe ser capaz de crear tareas de desinstalación del propio antivirus y de antivirus de terceros. 15.La solución y/o producto ofertado debe permitir la generación de reportes gráficos y personalización de estos. 16.Los reportes de la solución y/o producto ofertado deben ser fácilmente exportables en formatos CSV, PDF. 17.La solución y/o producto ofertado 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. 18.La solución y/o producto ofertado debe ser capaz de generación de alertas ante un evento específico mediante el envío de un correo. 19.Las actualizaciones de la solución y/o producto ofertado 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. 20.La solución y/o producto ofertado 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. 21.La solución y/o producto ofertado 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. 22.La solución y/o producto ofertado deberá permitir la ejecución		

SOLICITUD DE COTIZACIÓN

UNIDAD EJECUTORA : 312 GOB. REG. DPTO. CUSCO - UGEL CUSCO
NRO. IDENTIFICACIÓN : 001644

Señores	:			**R.U.C.**	
Dirección	:				
Teléfono	:		**Fax** :		
Nro. Cons.	: 136		**Fecha** : 25/09/2023	**Documento** :	
Concepto	:				

CANTIDAD REQUERIDA	UNIDAD MEDIDA	DESCRIPCION	PRECIO UNITARIO	PRECIO TOTAL
		TÉRMINO DE REFERENCIA: remota de scripts, batch files y paquetes personalizados de terceros a través de la consola. 23.La solución y/o producto ofertado deberá permitir generar grupos de clientes dinámicos y grupos estáticos. E.OTROS a.El fabricante deberá tener soporte técnico en español y laboratorio de análisis de malware en Sudamérica para atender incidencias que afecten la región. b.El fabricante deberá ocupar una posición de Leader o Challenger en el Cuadrante Mágico de Gartner del último año de publicación. c.El proveedor deberá brindar un SOC, cuya finalidad es brindar servicios horizontales para la UGEL CUSCO, en el ámbito de la ciberseguridad con lo que se busca conseguir lo siguientes puntos: -Incrementar la capacidad de vigilancia y detección de amenazas en las actividades diarias de los sistemas de información de UGEL CUSC -Analizar los ataques o posibles amenazas. -Gestión de las vulnerabilidades. -Mejorar la capacidad de respuesta ante cualquier ataque. d.El fabricante deberá emitir un certificado de las licencias adquiridas.		
			TOTAL	

Las cotizaciones deben estar dirigidas a GOB. REG. DPTO. CUSCO - UGEL CUSCO
en la siguiente dirección: AV. CAMINO REAL 114 Teléfono: 244494

Condiciones de Compra
- **Forma de Pago:**
- **Garantía:**
- **La Cotización** debe incluir el I.G.V.
- **Plazo de Entrega/ Ejecución del Servicio :**
- **Tipo de Moneda :**
- **Validez de la cotización :**
- **Remitir** junto con **su cotización** la Declaración Jurada y **Pacto de Integridad, debidamente firmadas y selladas.**
- **Indicar su razón social, domicilio fiscal y número de RUC**

Atentamente,

MINISTERIO DE EDUCACION DRE - CUSCO UGEL CUSCO

Area de compras

ESPECIFICACIONES TECNICAS PARA LA ADQUISICION DE LICENCIAS CORPORATIVAS DE SOFTWARE ANTIVIRUS

1. UNIDAD O ÁREA QUE REQUIERE LA ADQUISICIÓN.

Oficina de Informática – UGEL Cusco.

2. OBJETO DE LA ADQUISICIÓN.

Adquirir software antivirus que brinde protección a 113 estaciones de trabajo y 5 servidores pertenecientes a la UGEL CUSCO. De esta manera se busca garantizar la integridad de la información y servicios que están alojados en estos equipos, evitando la infiltración de software malicioso o cualquiera de sus variantes, alineándose a la protección de la información en los equipos servidores y estaciones de trabajo, que permita controlar y evaluar la infección de archivos, garantizando la continuidad de los principales sistemas y equipos de computo de la Institución.

3. FINALIDAD PÚBLICA.

Contribuir a minimizar el riesgo de pérdida, eliminación y daño de los archivos almacenados en los equipos informáticos de la UGEL CUSCO permitiendo a los funcionarios y trabajadores, el desarrollo normal de sus actividades operativas y administrativas, al reducir el tiempo de indisponibilidad en el uso de sus archivos y herramientas de trabajo.

4. REQUERIMIENTO

CANTIDAD	DESCRIPCION TECNICA
05 licencias	Servidores Windows 2012 – 2019, CentOS
113 licencias	Computadoras para los Usarios Clientes con Sistema Operativo Windows 7, 8, 10 Y 11

5. DESCRIPCIÓN BÁSICA DE LAS CARACTERÍSTICAS DEL BIEN CARACTERÍSTICAS Y CONDICIONES.

ESPECIFICACIONES TECNICAS DEL ANTIVIRUS

SOLUCIÓN DE PROTECCIÓN PARA ESTACIONES DE TRABAJO.

1. La solución y/o producto ofertado (en sus últimas versiónes) deberá ser compatible con los siguientes sistemas operativos: Microsoft® Windows® 11/10/8.1/8/7. 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, CentOS y superior.
2. La solución y/o 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.
3. La solución y/o 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.

4. La solución y/o 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.
5. La solución y/o producto ofertado debe ser capaz de detectar todo tipo de amenazas, entre los más comunes: virus, gusanos, troyanos, spyware, adware, rootkits, bots, ransomware, etc.
6. La solución y/o producto ofertado deberá contar con una funcionalidad antiransomware.
7. La solución y/o 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.
8. La solución y/o producto ofertado 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.
9. La solución y/o producto ofertado debe permitir elegir las unidades a escanear para los escaneos bajo demanda.
10. La solución y/o producto ofertado debe ser capaz de crear exclusiones de escaneo ya sea por archivo, extensión o carpeta específica.
11. La solución y/o producto ofertado debe pedir una contraseña ante intentos de cambio indebidos en la configuración del producto.
12. La solución y/o producto ofertado 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.
13. La solución y/o 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.
14. La solución y/o producto ofertado debe tener una funcionalidad en donde todas las ventanas emergentes se deshabiliten y la proteccion del sistema seguirá ejecutándose en segundo plano, pero no requerirá ninguna interacción por parte del usuario.
15. La solución y/o 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.
16. La solución y/o producto ofertado debe tener sistema de prevención de intrusiones basado en el host, (HIPS).
17. El sistema HIPS de la solución y/o producto ofertado debe tener los siguientes modos de configuración: automático, inteligente, interactivo, basado en políticas y aprendizaje.
18. La solución y/o producto ofertado debe poseer un firewall bidireccional que posea mínimo 4 modos de filtrado entre ellos, automático, interactivo,

aprendizaje y modo basado en políticas, además que pueda tener la capacidad de bloquear conexiones entrantes y salientes.

19. La solución y/o producto ofertado debe tener la capacidad de tener un filtro web con un mínimo de 27 categorías entre las cuales se deba permitir o bloquear el acceso a las webs según el administrador lo disponga.
20. La solución y/o producto ofertado permitirá crear grupos que contengan varios vínculos URL para crear reglas de permiso y bloqueo a determinados sitios web.
21. El bloqueo web de la solución y/o producto ofertado deberá poder asignarse por un rango de tiempo, por grupo y por equipo.
22. La solución y/o producto ofertado debe tener un filtro antispam que permita integrarse con clientes como Microsoft Outlook. Esta funcionalidad debe permitir al usuario crear una lista negra o blanca de direcciones de correo.
23. La solución y/o producto ofertado deberá analizar protocolos de e-mail POP3, IMAP, MAPI.
24. La protección del correo electrónico en el cliente de la solución y/o producto ofertado debe permitir definir si se desea escanear sólo correo recibido, correo enviado o correo leído.
25. La solución y/o producto ofertado debe tener la capacidad de añadir una nota o etiqueta en los correos electrónicos recibidos o leídos.
26. La solución y/o producto ofertado 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.
27. La solución y/o producto ofertado debe tener un módulo de protección en tiempo real para el acceso a la web.
28. La solución y/o producto ofertado debe ser capaz de escanear a través del protocolo SSL (HTTPS), de manera que se pueda impedir la descarga de archivos infectados.
29. La solución y/o producto ofertado debe de permitir realizar exclusiones de URL para que no sean analizadas por el antivirus tanto en el protocolo HTTP, y HTTPS.
30. La solución y/o 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.
31. La solución y/o 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).
32. La solución y/o producto ofertado debe ser capaz de crear CD's, ISO's o USB de rescate, que permitan escanear los equipos Microsoft.
33. La solución y/o producto ofertado 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.

34. La solución y/o producto ofertado 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.
35. La solución y/o 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).
36. La solución y/o producto ofertado deberá poder realizar exploraciones en estado inactivo para poder brindar de esa forma, una protección proactiva mientras el equipo no está en uso.
37. La solución y/o producto ofertado debe contar con la funcionalidad de bloqueo de exploits, que evite la explotación de vulnerabilidades en las aplicaciones.
38. La solución y/o producto ofertado debe contar con un modo transparente de uso, en el cual no muestre ninguna alerta cuando se esté ejecutando una aplicación en pantalla completa.
39. La solución y/o producto ofertado 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.
40. La solución y/o producto ofertado 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)
41. La solución y/o producto ofertado deberá contar con un módulo de protección contra Botnets, este módulo debe ser capaz de detectar conexiones con servidores maliciosos.
42. La solución y/o producto ofertado 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.
43. La solución y/o producto ofertado incluirá una protección con el teclado, contra registradores de pulsaciones.

A. SOLUCIÓN DE PROTECCIÓN PARA SERVIDORES

Se debe considerar La solución y/o producto ofertado (en sus últimas versiónes), para todos los servidores, con las siguientes características:

1. La solución y/o producto ofertado debe poder instalarse en su última versión, sobre plataformas Windows 2008 Server R2 SP1, small business server 2011(x64), Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022 y Server Core (Windows Server 2008 R2 SP1 Windows Server

2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 y Windows Server 2022)

2. La solución y/o producto ofertado debe poder instalarse sobre plataformas de x64 bits RedHat Enterprise Linux (RHEL) 7 y 8; CentOS 7 y 8; Ubuntu Server 16.04, 18.04 y 20.04 LTS; Debian10 y 11; SUSE Linux Enterprise Server (SLES) 12 y 15.
3. La solución y/o producto ofertado debe ser compatible con versiones del kernel del sistema operativo Linux 3.10.0 y posteriores
4. La solución y/o producto ofertado debe contar con un módulo de detección en tiempo real que proteja contra códigos maliciosos en cada acción realizada en el equipo (abrir, crear o ejecutar)
5. La solución y/o producto ofertado debe ser capaz de detectar todo tipo de amenazas, entre los más comunes: virus, gusanos, troyanos, spyware, adware, rootkits, bots, ransomware, etc.
6. La solución y/o producto ofertado deberá contar con una funcionalidad antiransomware.
7. La solución y/o producto ofertado 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.
8. La solución y/o producto ofertado para servidores Windows deberá contar con exclusiones automáticas que permitan detectar las aplicaciones críticas del servidor y los archivos críticos del sistema operativo y los agregue automáticamente a la sección de exclusiones al momento de ser instalado.
9. La solución y/o producto ofertado debe ser capaz de crear exclusiones de escaneo ya sea por archivo, extensión o carpeta específica.
10. La solución y/o producto ofertado debe pedir una contraseña ante intentos de cambio indebidos en la configuración del producto.
11. La solución y/o producto ofertado debe contar con un agente que le permita ser administrado desde una consola centralizada.
12. La solución y/o producto ofertado debe permitir generar dentro de la misma solución antivirus repositorios de actualización, los cuales deberán ser distribuidas mediante protocolo http localmente, esto sin depender de aplicaciones externas o de la consola de Administración.
13. La protección en tiempo real de la solución y/o producto ofertado debe iniciarse con el sistema operativo, así como poder definir qué tipos de medios serán analizados por el módulo.
14. La solución y/o producto ofertado debe tener sistema de prevención de intrusiones basado en el host, (HIPS).
15. El sistema HIPS de la solución y/o producto ofertado debe tener los siguientes modos de configuración: automático, inteligente, interactivo, basado en políticas y aprendizaje.
16. La solución y/o producto ofertado debe permitir escanear archivos comprimidos.

17. La solución y/o producto ofertado debe permitir elegir las unidades a escanear para los escaneos bajo demanda.
18. En sistemas operativos Windows, la solución y/o producto ofertado deberá contar con una herramienta integrada que permita inspeccionar completamente componentes del sistema (Controladores, Aplicaciones Instaladas, Conexiones de Red y entradas importantes del Registro de Windows), esto con la finalidad de determinar la causa de comportamientos sospechosos en el sistema que puede deberse a incompatibilidad de software, hardware o código malicioso.
19. La solución y/o producto ofertado debe tener un caché local para aumentar el rendimiento de los entornos virtuales, garantizando que el archivo sólo se explora una vez.

B. SANDBOXING.

1. Uso de Sandboxing en la nube para analizar el comportamiento de archivos, con SLA de 5 minutos hasta 1 hora de respuesta.
2. Es posible crear una exclusión por ruta, detección y su hash (SHA-1)
3. Capacidad de sincronizar su licenciamiento con la nube y la consola de administración en sitio o en la nube.
4. Detectar un archivo sospechoso ejecutado por primera vez se debe mostrar una advertencia, si el análisis se completa antes de ejecutar el archivo por primera vez, no se muestra el aviso archivo en análisis.
5. Debe borrar automáticamente las muestras de los archivos/ejecutables en los servidores donde fue analizado el comportamiento.
6. Capacidad para enviar correos SPAM para su análisis.
7. Debe tener únicamente estos umbrales de detección: desconocido, limpio, sospechoso, altamente sospechoso y malicioso.
8. Debe tener la siguiente información de un archivo enviado al Sanboxing en la nube: nombre del equipo desde donde se ingresó el archivo, el usuario que lo ingresó, la razón, hash en SHA-1, nombre del archivo ingresado, tamaño del archivo, categoría.
9. Debe tener protección proactiva, es decir, que el archivo/ejecutable sea bloqueado hasta recibir el resultado del Sandbox en la nube.
10. Se debe tener capacidad para integrarse con la solución de antivirus o protección del punto final, para tener mayores posibilidades de protección y aplicación de políticas.
11. Enviar un archivo/ejecutable a través de una consola de administración del punto final.

C. CIFRADO DE DISCO.

1. La solución y/o producto ofertado deberá ser capaz de cifrar los Endpoints deseados desde el inicio de sistema.
2. La solución y/o producto ofertado deberá disponer de diversas posibilidades de recuperación de Passwords para usuarios remotos que se vean bloqueados.

3. La solución y/o producto ofertado deberá poder programar las tareas de cifrado sobre los Endpoints deseados con la posibilidad de pausar la ejecución para retomar luego desde el último punto.
4. La solución y/o producto ofertado deberá poder ser administrada desde la misma consola central junto con las otras soluciones descriptas en el TDR.

D. CONSOLA DE ADMINISTRACIÓN CENTRALIZADA DE LA SOLUCIÓN Y/O PRODUCTO OFERTADO

1. 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.
2. La consola de administración debe permitir la configuración y administración remota de la solución y/o producto ofertado, instalada en las estaciones de trabajo y servidores (Windows, Linux, Mac). Soporte para dispositivos móviles.
3. 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.
4. 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.
5. 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.
6. La consola de acceso al servidor deberá ser 100% web, siendo compatible con los siguientes navegadores: Mozilla Firefox, Microsoft SCCM, Google Chrome, Safari, Opera.
7. 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.
8. 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.
9. El producto debe ser capaz de mostrar los equipos detectados en la red.
10. La consola de administración centralizada debe tener la capacidad de mostrar los intentos de infección de virus en los equipos clientes.
11. La solución y/o producto ofertado 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.
12. La solución y/o producto ofertado 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.

13. La solución y/o producto ofertado debe permitir la instalación y desinstalación remota de los servidores y clientes antivirus.
14. La solución y/o producto ofertado debe ser capaz de crear tareas de desinstalación del propio antivirus y de antivirus de terceros.
15. La solución y/o producto ofertado debe permitir la generación de reportes gráficos y personalización de estos.
16. Los reportes de la solución y/o producto ofertado deben ser fácilmente exportables en formatos CSV, PDF.
17. La solución y/o producto ofertado 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.
18. La solución y/o producto ofertado debe ser capaz de generación de alertas ante un evento específico mediante el envío de un correo.
19. Las actualizaciones de la solución y/o producto ofertado 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.
20. La solución y/o producto ofertado 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.
21. La solución y/o producto ofertado 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.
22. La solución y/o producto ofertado deberá permitir la ejecución remota de scripts, batch files y paquetes personalizados de terceros a través de la consola.
23. La solución y/o producto ofertado deberá permitir generar grupos de clientes dinámicos y grupos estáticos.

E. OTROS

a. El fabricante deberá tener soporte técnico en español y laboratorio de análisis de malware en Sudamérica para atender incidencias que afecten la región.
b. El fabricante deberá ocupar una posición de Leader o Challenger en el Cuadrante Mágico de Gartner del último año de publicación.
c. El proveedor deberá brindar un SOC , cuya finalidad es brindar servicios horizontales para la UGEL CUSCO, en el ámbito de la ciberseguridad con lo que se busca conseguir lo siguientes puntos:
   - Incrementar la capacidad de vigilancia y detección de amenazas en las actividades diarias de los sistemas de información de UGEL CUSCO

- Analizar los ataques o posibles amenazas.
- Gestión de las vulnerabilidades.
- Mejorar la capacidad de respuesta ante cualquier ataque.

d. El fabricante deberá emitir un certificado de las licencias adquiridas.

6. ACONDICIONAMIENTO O INSTALACIÓN

- La implementación de la solución propuesta no excederá de siete días (07) calendarios.
- La solución ofertada, incluirá la configuración de la consola de administración.
- En lo posible la puesta en servicio de la solución ofertada se realizará sin afectar las labores normales de la institución y sin interrumpir la normal provisión de los servicios.
- Preparar la configuración de la consola o de paquetes de instalación para los equipos de las sedes remotas.
- El postor ganador presentará un plan de despliegue de la solución dentro de los cinco días calendarios posteriores a la firma del contrato.
- Toda coordinación sobre la instalación y/o configuración de la solución será coordinada directamente con la Oficina de Informatica.

7. DEL POSTOR

El postor deberá contar con UN (01) profesional certificado en la solución ofertada. La certificación deberá ser otorgada por el fabricante de la solución propuesta (adjuntar copia de su certificado para su respectiva validación).

8. PRESTACIONES ACCESORIAS

Soporte Técnico

El postor ganador ofrecerá canales de comunicación (telefónicamente y correo electrónico) para el reporte de incidencias.

La UGEL CUSCO notificará las anomalías que se presenten incluyendo la siguiente información:

- Fecha y hora
- Descripción del problema y servicios afectados
- Persona de contacto del UGEL CUSCO.

Ante cada reporte de anomalías, el postor ganador deberá realizar y presentar a la UGEL CUSCO un informe (por correo electrónico) que contendrá por lo menos la siguiente información:

- Descripción detallada del problema, su causa y solución encontrada.
- Personal asignado para la resolución del mismo.
- Problemas presentados durante resolución.
- Documentación adjunta de los cambios hechos.
- Recomendaciones
- Fecha y hora de resolución.

Capacitación

- La empresa proveedora deberá brindar capacitación sobre el uso de las herramientas administrativas del software y la configuración de cada producto de la solución entregada, según perfil del usuario (Administrdores y Soporte Tecnico)
- Se requiere curso con contenido oficial del fabricante, en la solución de antivirus adquirida.
- Los cursos deberán ser dictados por un especialista en la herramienta ofertada y para un mínimo de seis (06) personas.
- La fecha de inicio de la capacitación será programada a partir del quinto dia calendario posterior a la firma del contrato y el tiempo de capacitación será de 06 horas.

9. REQUISITOS DE CALIFICACIÓN:

a) Requisitos:
Documento que acredite fehacientemente la representación de quien suscribe la oferta.

b) Acreditación:
En caso de persona natural y/o jurídica presentar copia del documento nacional de identidad (DNI) o documento análogo, copia de Registro Nacional de Proveedores **(RNP)** y ficha RUC.

c) Experiencia del Postor:
El postor debe acreditar mínimo tres (03) contrataciones, por la venta de bienes iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.
Se consideran bienes iguales o similares a los siguientes: venta de software, licencias de software, antivirus otros similares.

10. PLAZO DE ENTREGA

El plazo máximo de entrega es de 07 días calendarios, contados a partir del día siguiente de la firma del contrato u orden de compra, este plazo incluye la entrega de las licencias, un documento que acredite a la UGEL CUSCO como propietario de las mismas, configuración de la consola de administración y la instalación o habilitación del software en los equipos informáticos de la sede Central o sedes remotas de la UGEL CUSCO, que designe la Oficina de Informatica.

11. FORMA DE ENTREGA

La entrega debe ser total, de acuerdo al plazo fijado en las instalaciones de la Oficina de Almacen de la UGEL Cusco, cito en Av. Camino Real #114 - Cusco.

12. GARANTÍA COMERCIAL DEL BIEN

Las licencias, funcionalidad, actualizaciones y mejoras, tendrán una garantía de 1 año, tiempo que durará el acceso al soporte técnico ofrecido por la marca ofertada o el proveedor.

Todos los bienes suministrados serán en sus ultimas versiónes las cuales incorporan todas las mejoras en cuanto a funcionalidad y prestaciones.

La UGEL CUSCO notificará al postor ganador cualquier defecto o mal funcionamiento del producto inmediatamente después de haberlo descubierto, el postor ganador tendrá la oportunidad para inspeccionar el defecto o mal funcionamiento y proceder a la subsanación sin costo a la entidad, cuando se determine que el problema se debe a un error propio del bien.

13. FORMA DE PAGO

Se realizará un pago único, posterior a la conformidad de la recepción de todos los bienes o servicios requeridos en el presente documento.

14. CONFORMIDAD DE RECEPCIÓN DEL BIEN

La conformidad será emitida por cada área usuaria previo informe técnico de la Oficina de Informática.

15. RESPONSABILIDAD DEL CONTRATISTA

El contratista es el responsable por la calidad ofrecida y por los vicios ocultos de los bienes o servicios ofertados por un plazo no menor de un (1) año contado a partir del día siguiente de la firma del contrato, el cual podrá establecer excepciones para bienes fungibles y/o perecibles, siempre que la naturaleza de estos bienes no se adecúe a este plazo.

16. PENALIDAD.

La aplicación de penalidades por retraso injustificado en la atención del servicio requerido, será aplicado en base al marco normativo vigente de la Ley de Contrataciones del Estado y su reglamento vigente.

GOBIERNO REGIONAL CUSCO
DIRECCIÓN REGIONAL DE EDUCACIÓN CUSCO
UNIDAD DE GESTIÓN EDUCATIVA LOCAL CUSCO
Ing. Yolvi Quispe Rocca
RESPONSABLE DEL EQUIPO DE INFORMATICA

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"AÑO DEL FORTALECIMIENTO DE LA SOBERANÍA NACIONAL"

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 .....declaro bajo juramento:

1. **No tener impedimento para contratar con el Estado**, conforme al artículo 11° de la Ley N° 30225, Ley de Contrataciones del Estado.
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 de Contrataciones del Estado y su Reglamento, así como en la Ley N° 27444, Ley del Procedimiento Administrativo General.
6. Actuaré conforme a los principios previstos en la Ley de Contrataciones del Estado.

Cusco, de del 2023

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

*DNI N° :*_____

*RUC N:*_____

Importante:
De acuerdo a lo indicado en el artículo 44° de la Ley de Contrataciones, la Entidad puede declarar la nulidad de oficio, de las Órdenes de Compra o Servicios, si se contraviene lo indicado en la presente Declaración Jurada

ANEXO N°02:
DECLARACIÓN JURADA DEL PROVEEDOR

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

Presente. -
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 funcionarios 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 a las que se refiere al artículo 7 del reglamento de la ley de contrataciones del estado, ofrecido, negociado o efectuado, cualquier pago o, en general, cualquier beneficio o incentivo ilegal en relación al contrato u orden de compra y servicio.
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 a las que se refiere al artículo 7 del reglamento de la ley de contrataciones del estado.

Cusco, de del 2023.

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