SOLICITUD DE COTIZACIÓN

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

Señores : **R.U.C.**
Dirección :
Teléfono : **Fax** :
Nro. Cons. : 14 **Fecha** : 18/04/2023 **Documento** Pedido de compra consolidado
Concepto : **adquisicion de software corporativo antivirus de las diferentes oficinas del ambito de la ugel cusco.**

CANTIDAD REQUERIDA	UNIDAD MEDIDA	DESCRIPCION	PRECIO UNITARIO	PRECIO TOTAL
113.00	UNIDAD	SOFTWARE ANTIVIRUS TÉRMINO DE REFERENCIA. UNIDAD O AREA QUE REQUIERE LA ADQUISICION: OFICINA DE INFORMATICA DESCRIPCION TECNICA: LICENCIA CLIENTE: CANTIDAD (5) CINCO usuarios clientes con sistema operativo Windows 7,8,10 Y 11 ESPECIFICACIONES: ESPECIFICACIONES ADJUNTO AL PEDIDO UNIDAD O AREA QUE REQUIERE LA ADQUISICION: OFICINA DE ABASTECIMIENTO DESCRIPCION TECNICA: LICENCIA CLIENTE: CANTIDAD 06 usuarios clientes con sistema operativo Windows 7,8,10 Y 11 ESPECIFICACIONES: ESPECIFICACIONES ADJUNTO AL PEDIDO UNIDAD O AREA QUE REQUIERE LA ADQUISICION: OFICINA DE ADMINISTRACION DESCRIPCION TECNICA: LICENCIA CLIENTE: CANTIDAD 02 usuarios clientes con sistema operativo Windows 7,8,10 Y 11 ESPECIFICACIONES: ESPECIFICACIONES ADJUNTAS AL PEDIDO UNIDAD O AREA QUE REQUIERE LA ADQUISICION: DIRECCION DE GESTION INSITUCIONAL DESCRIPCION TECNICA: LICENCIA CLIENTE: CANTIDAD 11 usuarios clientes con sistema operativo Windows 7,8,10 Y 11 ESPECIFICACIONES: ESPECIFICACIONES ADJUNTAS AL PEDIDO UNIDAD O AREA QUE REQUIERE LA ADQUISICION: DIRECCION DE GESTION PEDAGOGICA DESCRIPCION TECNICA: LICENCIA CLIENTE: CANTIDAD 20 usuarios clientes con sistema operativo Windows 7,8,10 Y 11 ESPECIFICACIONES: ESPECIFICACIONES ADJUNTO AL PEDIDO		

MINISTERIO DE EDUCACION DRE - CUSCO OFICINA ABASTECIMIENTO DIRECCIÓN ADMINISTRACIÓN UGEL CUSCO

SOLICITUD DE COTIZACIÓN

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

Señores :
R.U.C.
Dirección :
Teléfono :
Fax :
Nro. Cons. : 14
Fecha : 18/04/2023
Documento :
Concepto :

CANTIDAD REQUERIDA	UNIDAD MEDIDA	DESCRIPCION	PRECIO UNITARIO	PRECIO TOTAL
		TÉRMINO DE REFERENCIA: UNIDAD O AREA QUE REQUIERE LA ADQUISICION: OFICINA DE ALMACEN DESCRIPCION TECNICA: LICENCIA CLIENTE: CANTIDAD 04 usuarios clientes con sistema operativo Windows 7,8,10 Y 11 ESPECIFICACIONES: ESPECIFICACIONES ADJUNTAS AL PEDIDO UNIDAD O AREA QUE REQUIERE LA ADQUISICION: CONVIVENCIA ESCOLAR DESCRIPCION TECNICA: LICENCIA CLIENTE: CANTIDAD 02 usuarios clientes con sistema operativo Windows 7,8,10 Y 11 ESPECIFICACIONES: ESPECIFICACIONES ADJUNTAS AL PEDIDO UNIDAD O AREA QUE REQUIERE LA ADQUISICION: DIRECCION DESCRIPCION TECNICA: LICENCIA CLIENTE: CANTIDAD 02 usuarios clientes con sistema operativo Windows 7,8,10 Y 11 ESPECIFICACIONES: ESPECIFICACIONES ADJUNTAS AL PEDIDO UNIDAD O AREA QUE REQUIERE LA ADQUISICION: ESCALAFON DESCRIPCION TECNICA: LICENCIA CLIENTE: CANTIDAD 06 usuarios clientes con sistema operativo Windows 7,8,10 Y 11 ESPECIFICACIONES: ESPECIFICACIONES ADJUNTAS AL PEDIDO UNIDAD O AREA QUE REQUIERE LA ADQUISICION: SUPERVISION DE II.EE DESCRIPCION TECNICA: LICENCIA CLIENTE: CANTIDAD 04 usuarios clientes con sistema operativo Windows 7,8,10 Y 11 ESPECIFICACIONES: ESPECIFICACIONES ADJUNTAS AL PEDIDO		

MINISTERIO DE EDUCACION DIRE - CUSCO OFICINA ABASTECIMIENTO DIRECCIÓN ADMINISTRACIÓN UGEL CUSCO

SOLICITUD DE COTIZACIÓN

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

Señores :
R.U.C.
Dirección :
Teléfono :
Fax :
Nro. Cons. : 14
Fecha : 18/04/2023
Documento :
Concepto :

CANTIDAD REQUERIDA	UNIDAD MEDIDA	DESCRIPCION	PRECIO UNITARIO	PRECIO TOTAL
		TÉRMINO DE REFERENCIA: UNIDAD O AREA QUE REQUIERE LA ADQUISICION: OFICINA DE CONTROL INTERNO DESCRIPCION TECNICA: LICENCIA CLIENTE: CANTIDAD 03 usuarios clientes con sistema operativo Windows 7,8,10 Y 11 ESPECIFICACIONES: ESPECIFICACIONES ADJUNTO SEGUN PEDIDO UNIDAD O AREA QUE REQUIERE LA ADQUISICION: COMISION PERMANENTE DE PROCESOS ADMINISTRATIVOS DISCIPLINARIOS DESCRIPCION TECNICA: LICENCIA CLIENTE: CANTIDAD 03 usuarios clientes con sistema operativo Windows 7,8,10 Y 11 ESPECIFICACIONES: ESPECIFICACIONES ADJUNTAS SEGUN PEDIDO UNIDAD O AREA QUE REQUIERE LA ADQUISICION: CONTROL PATRIMONIAL DESCRIPCION TECNICA: LICENCIA CLIENTE: CANTIDAD 02 usuarios clientes con sistema operativo Windows 7,8,10 Y 11 ESPECIFICACIONES: ESPECIFICACIONES ADJUNTO SEGUN PEDIDO UNIDAD O AREA QUE REQUIERE LA ADQUISICION: OFICINA DE PERSONAL DESCRIPCION TECNICA: LICENCIA CLIENTE: CANTIDAD 12 usuarios clientes con sistema operativo Windows 7,8,10 Y 11 UNIDAD O AREA QUE REQUIERE LA ADQUISICION: OFICINA DE REMUNERACIONES DESCRIPCION TECNICA: LICENCIA CLIENTE: CANTIDAD 09 usuarios clientes con sistema operativo Windows 7,8,10 Y 11 ESPECIFICACIONES: ESPECIFICACIONES ADJUNTAS SEGUN PEDIDO		

MINISTERIO DE EDUCACION DRE - CUSCO OFICINA ABASTECIMIENTO DIRECCIÓN ADMINISTRACIÓN UGEL CUSCO

SOLICITUD DE COTIZACIÓN

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

Señores	:				**R.U.C.**
Dirección	:				
Teléfono	:		**Fax**	:	
Nro. Cons.	: 14		**Fecha** : 18/04/2023	**Documento** :	
Concepto	:				

CANTIDAD REQUERIDA	UNIDAD MEDIDA	DESCRIPCION	PRECIO UNITARIO	PRECIO TOTAL
		TÉRMINO DE REFERENCIA: UNIDAD O AREA QUE REQUIERE LA ADQUISICION: OFICINA DE TESORERIA DESCRIPCION TECNICA: LICENCIA CLIENTE: CANTIDAD 04 usuarios clientes con sistema operativo Windows 7,8,10 Y 11 ESPECIFICACIONES: ESPECIFICACIONES ADJUNTO SEGUN PEDIDO UNIDAD O AREA QUE REQUIERE LA ADQUISICION: TRAMITE DOCUMENTARIO DESCRIPCION TECNICA: LICENCIA CLIENTE: CANTIDAD 05 usuarios clientes con sistema operativo Windows 7,8,10 Y 11 UNIDAD O AREA QUE REQUIERE LA ADQUISICION: AREA DE ASESORIA LEGAL DESCRIPCION TECNICA: LICENCIA CLIENTE: CANTIDAD 05 usuarios clientes con sistema operativo Windows 7,8,10 Y 11 ESPECIFICACIONES: ESPECIFICACIONES ADJUNTO SEGUN PEDIDO ESPECIFICACIONES TE QUE REQUIERE LA ADQUISICION: SERVIDORES - INFORMATICA DESCRIPCION TECNICA LICENCIA SERVIDORES DE INFORMATICA: CANTIDAD (5) CINCO Servidores - Windows Server 2016 -2019, CentOS LICENCIA PARA COMPUTADORAS DE INFORMATICA: USUARIOS CLIENTES CON SISTEMA OPERATIVO WINDOWS 7,8,10 Y 11 SE ADJUNTA LAS ESPECIFICACIONES TECNICAS UNIDAD O AREA QUE REQUIERE LA ADQUISICION: CONTABILIDAD DESCRIPCION TECNICA: LICENCIA CLIENTE: CANTIDAD 02 usuarios clientes con sistema operativo Windows 7,8,10 Y 11 ESPECIFICACIONES: ESPECIFICACIONES ADJUNTAS AL PEDIDO		

SOLICITUD DE COTIZACIÓN

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

Señores	:			**R.U.C.**	
Dirección	:				
Teléfono	:	**Fax**	:		
Nro. Cons.	: 14	**Fecha** :	18/04/2023	**Documento** :	
Concepto	:				

CANTIDAD REQUERIDA	UNIDAD MEDIDA	DESCRIPCION	PRECIO UNITARIO	PRECIO TOTAL
		TÉRMINO DE REFERENCIA: UNIDAD O AREA QUE REQUIERE LA ADQUISICION: CONSTANCIA DE PAGOS DESCRIPCION TECNICA: LICENCIA CLIENTE: CANTIDAD 01 usuarios clientes con sistema operativo Windows 7,8,10 Y 11 ESPECIFICACIONES: ESPECIFICACIONES ADJUNTA SEGUN PEDIDO		
			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 EDUCACIÓN DRE - CUSCO OFICINA ABASTECIMIENTO UGEL CUSCO

Area de Logistica

ESPECIFICACIONES TECNICAS
ADQUISICION DE LICENCIAS CORPORATIVAS DE ANTIVIRUS

1. UNIDAD O ÁREA QUE REQUIERE LA ADQUISICIÓN
Oficina de Informática

2. OBJETO DE LA ADQUISICIÓN
Adquirir software corporativo de antivirus que brinde protección a 108 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 las operaciones 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 Server 2016 – 2019, CentOS
108 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.

5.1. PLATAFORMA
- Se requiere una solución basada en la nube.
- Todas las conexiones al almacén de datos deben ser auditadas, cifradas y los datos almacenados deben ser "seudonimizados" antes de ser procesados por tareas automatizadas.
- La plataforma de gestión deberá tener las siguientes certificaciones:
  - 27001 ISO
  - 27018 ISO
  - RGPD
- Deberá proporcionar desde la nube el conjunto de servidores y bases de datos para procesar información relacionada con el servicio. Los procesos capturados desde los puntos finales se manejarán en la nube para que el impacto en los sistemas empresariales sea mínimo.

5.2. CONSOLA DE ADMINISTRACIÓN
- Los administradores de servicios deberán poder administrar de forma centralizada en una sola consola la seguridad y la productividad de todas las estaciones de trabajo y servidores Windows, incluidos los portátiles y las oficinas remotas, desde cualquier navegador web.

- Deberá ser una consola web adaptable para ser utilizada desde cualquier dispositivo, incluyendo smartphones y tabletas.
- La consola de administración deberá admitir los siguientes navegadores web:
  - Chrome
  - Internet Explorer
  - Microsoft Edge
  - Firefox
  - Ópera
- No deberá haber límite en el número de dispositivos que administrará la consola.
- Deberá proporcionar una interfaz donde se puedan consultar los datos en tiempo real.
- Deberá tener información procesable del panel y filtros para los períodos del último año, mes, 7 días y 24 horas.
- Deberá permitirle seleccionar la información del panel por grupos y subgrupos de extremos.
- Deberá tener en la página detalles/información de los equipos un panel individual del punto final seleccionado que muestre todas las detecciones e indicadores de ataque.
- Deberá tener un panel que proporcione visibilidad de los indicadores de ataque (IOA) detectados con widgets sobre el número de eventos, indicadores e indicadores de ataque.
- Los indicadores de ataque (IOA) deberán asignarse a una táctica y técnica de la matriz MITRE ATT&CK.
- Deberá permitirle identificar la etapa del ataque y sus características.
- Deberá tener información sobre las recomendaciones para las respuestas personalizadas y permitirle tomar medidas de contención y remediación.
- Deberá tener el final directo de la información extendida sobre un indicador de ataque con enlaces desde el sitio web de MITRE.
- Deberá permitir habilitar y configurar la detección de IOAs.
- Deberá mostrar todos los IOAs detectados en la red.
- Deberá encontrar todos los equipos con un IOA específico.
- Deberá encontrar todos los IOAs detectados en un equipo.
- Deberá encontrar computadoras y IOAs relacionadas.
- Deberá permitirle archivar uno o más indicadores de ataque.
- Deberá permitirle marcar uno o más IOAs como pendientes.
- Deberá proporcionar detalles de un IOA y recomendaciones de respuesta.
- Deberá tener una investigación automática de usuarios y computadoras comprometidos, para determinar la causa raíz del ataque, proporcionar información como URL y direcciones IP involucradas, y con una visión general del impacto general del ataque.
- Deberá tener imágenes de ataque con información forense sobre procesos, comunicaciones y comandos sobre malware, exploits, IOAs y PUPs.
- Deberá permitirle interactuar con los elementos gráficos y realizar acciones en varios nodos simultáneamente y ver los detalles de la actividad de procesos específicos.

- Deberá generar información forense relacionada con cada equipo para que pueda ser explorada posteriormente.
- Deberá incluir un informe de amenazas detectadas que correlaciona las acciones que realizó el proceso o en el contexto involucrado, por ejemplo, si se descargó de Internet o se extrajo de un archivo comprimido.
- Deberá incluir informes de estado sobre protecciones, detecciones de malware y un informe ejecutivo con un resumen de la información global.
- Deberá permitir la descarga de informes y alertas, el acceso a la configuración y las actualizaciones disponibles del agente.
- Deberá permitirle generar informes inmediatamente con los datos o en tiempo real.
- Deberá permitir la programación y el envío periódico de informes por correo electrónico y en diferentes formatos para su posterior tratamiento.
- Deberá tener la capacidad de aplicar directivas en tiempo real a los puntos finales protegidos.
- Deberá permitirle crear máquinas caches para administrar las actualizaciones del agente/protección, con optimización del ancho de banda.
- Deberá permitir la búsqueda de nuevos puntos finales en la red que aún no tienen instalado el agente e instalar la protección de forma remota.
- Deberá establecer un número máximo de máquinas que estén activas simultáneamente para VDI no persistentes y, por lo tanto, controlar la concesión de licencias, así como el equipo activo.
- Deberá poder enviar alertas cuando:
  - Detecciones de malware
  - Análisis de exploits
  - Detecciones de phishing
  - Aplicación desconocida bloqueada
  - Programas bloqueados por el administrador
  - Bloqueo de una URL de malware
  - Bloqueo de un intento de intrusión
  - Dispositivos bloqueados
  - Indicadores de ataque (IOA)
  - Equipos con errores de protección
  - Equipos sin licencia
  - Errores de instalación
  - Detección de un equipo sin agente instalado
- Deberá permitir la aplicación de 2FA para usuarios de administración de consolas.
- Deberá tener un registro de actividad de los usuarios de administración de consola como desconectados con fecha, hora e IP, tareas, cambios de configuración y cambios en el sistema.
- Deberá tener información del hardware de los equipos como CPU, RAM, disco, BIOS y TPM.
- Deberá tener información del software instalado en los puntos finales, tales como el nombre del software, la versión y el historial de instalación y desinstalación.
- Deberá poder realizar cambios de configuración de forma granular y a nivel de extremo.

- Deberá poder establecer los tiempos de actualización tanto para el motor de protección de la solución como para las vacunas de firma.
- Deberá poder actualizar automáticamente tanto el motor de protección de la solución como los archivos locales (base de datos) de firmas de malware.
- Deberá permitirle crear tareas inmediatas para escanear los puntos finales, así como programar una tarea de análisis periódica diaria/semanal/mensual.
- Deberá tener información sobre el estado de las protecciones avanzadas EDR y Antivirus EPP, los archivos de firma de malware, las comunicaciones con los servidores de la solución en la nube y la última conectividad de punto final a la consola.
- Deberá poder realizar un servicio de detección de redes automáticamente para encontrar puntos en desarrollo no protegidos que no tengan el agente de solución.
- Debería poder crear listas de informes personalizadas con la siguiente información:
  - Licencias
  - Equipos no gestionados descubiertos
  - Ordenadores con nombre duplicado
  - Software
  - Hardware
  - Estado de protección del equipo
  - Actividad de malware y PUP
  - Actividad de explotación
  - Programas bloqueados
  - Amenazas detectadas por antivirus
  - Intentos de intrusión bloqueados
  - Dispositivos bloqueados
  - Indicadores de ataque (IOA)
  - Acceso web por categoría
  - Acceso web por ordenador
  - Programas bloqueados por el administrador
  - Informe Ejecutivo
- Deberá poder crear filtros personalizados para buscar información de puntos de conexión.
- Deberá introducir un mensaje descriptivo para informar a los usuarios del motivo de la alerta, mostrándose en una ventana emergente localmente con el texto configurado.

5.3. AGENTE DE LA INSTALACIÓN

- El agente implementado deberá permitir la comunicación y la administración de la protección antivirus tradicional (Endpoint Protection Platform o EPP), así como la protección avanzada de Endpoint Detection and Response (EDR).
- Deberá recopilar la información correspondiente a los eventos y los componentes que los producen, sin recopilar información ni documentos de usuario.
- La solución deberá poder implementarse de forma silenciosa mediante los siguientes mecanismos: paquete de instalación local, dirección URL

descargable, de forma remota a través de la consola de administración y GPO de Microsoft Active Directory.

- Deberá tener la capacidad para reinstalar el agente y reparar de forma remota los equipos con agentes que no se comunican con el servidor o que tienen errores de protección.
- Deberá tener la capacidad de desinstalar otras soluciones de seguridad de endpoints que estén instaladas.
- Deberá tener una contraseña contra la desinstalación y paralización del servicio.
- Deberá permitir que se deshabilite temporalmente la funcionalidad de la solución de forma granular, cuando sea necesario para fines de soporte y localmente, utilizando el conjunto de contraseñas.
- Deberá tener protección contra manipulaciones para la prevención de usuarios y malware, sin intentar cerrar protecciones y servicios.
- Deberá tener protección contra manipulaciones que utilice la tecnología ELAM (Early Launch Anti-Malware) incluida en los sistemas operativos Windows 10 y Server 2019 o superior.
- Deberá permitirle cambiar el idioma del agente.
- Deberá permitir ocultar el icono en la bandeja del sistema.
- Deberá permitir la configuración de la comunicación del agente en tiempo real con la consola de administración.
- Deberá ser capaz de realizar actualizaciones automatizadas por P2P, a través de Internet o a través de Servicios de Red (proxy).
- No se aceptarán soluciones compuestas por múltiples agentes. La solución deberá administrarse mediante un único agente instalado.
- Deberá ser capaz de gestionar de forma centralizada las instantáneas (Shadow Copies) en la consola del producto, para permitir ir restaurando versiones anteriores de archivos en caso de una infección de ransomware.
- Al habilitar las instantáneas (las instantáneas son tecnología incluida en Microsoft Windows) deberá especificar el porcentaje de espacio en disco que se utilizará para las instantáneas.
- Las instantáneas se deberán crear cada 24 horas y la solución debe ser capaz de retener hasta 7 copias a la vez.
- Las instantáneas deberán protegerse contra los ataques de ransomware con protección contra manipulaciones para evitar que el ransomware elimine las copias de seguridad en los dispositivos afectados antes de cifrar los archivos en el sistema.
- El agente debe ser compatible con los siguientes sistemas operativos:
  Microsoft Windows:
  - Windows XP SP3 (32 bits)
  - Windows Vista (32 bits y 64 bits)
  - Windows 7 (32 bits y 64 bits)
  - Windows 8 (32 bits y 64 bits)
  - Windows 8.1 (32 bits y 64 bits)
  - Windows 10 (32 bits y 64 bits)
  - Windows 10 (ARM)
  - Windows 11 (32 bits y 64 bits)
  - Windows 11 (ARM)

- Windows Server 2003 (32 bits, 64 bits y R2) SP2 y versiones posteriores
- Windows Server 2008 (32 bits y 64 bits) y 2008 R2
- Windows Small Business Server 2011, 2012
- Windows Server 2012 R2
- Windows Server 2016 y 2019
- Windows Server Core 2008, 2008 R2, 2012 R2, 2016 y 2019
- Windows Server 2022 (64 bits)
- Windows XP Embedded
- Windows Embedded para punto de servicio
- Windows Embedded POSReady 2009, 7, 7 (64 bits)
- Windows Embedded Standard 2009, 7, 7 (64 bits), 8, 8 (64 bits),
- Windows Embedded Pro 8, 8 (64 bits)
- Windows Embedded Industry 8, 8 (64 bits), 8.1, 8.1 (64 bits)
- Windows IoT Core 10, 10 (64 bits)
- Windows IoT Enterprise 10, 10 (64 bits)

Linux:

- RedHat 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 y 6.10 (32 bits)
- CentOS 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 y 6.10 (32 bits)
- Ubuntu 14.04 LTS, 14.10, 15.04, 15.10, 16.04 LTS, 16.10, 17.04, 17.10, 18.04 LTS, 19.04, 19.10, 20.04 LTS, 20.10, 21.04, 21.10 y 22.04 (64 bits)
- Fedora 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34 y 35 (64 bits).
- Debian 8, 9,10 y 11 (64 bits)
- RedHat 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9 y 6.10 (64 bits)
- RedHat 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 8, 8.0, 8.1, 8.2, 8.3 y 8.4 (64 bits)."
- CentOS 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 8, 8.0, 8.1, 8.2, 8.3, 8.4 y 8.5 (64 bits).
- LinuxMint 18, 18.1, 18.2, 18.3, 19, 19.1,19.2, 19.3, 20, 20.1, 20.2 y 20.3 (64 bits)
- Suse Linux Enterprise 11SP2, 11SP3, 11SP4, 12, 12SP1, 12SP2, 12SP3, 12SP4, 12SP5, 15, 15SP1, 15SP2 y 15SP3
- Oracle Linux 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 8.0, 8.1, 8.2, 8.3 y 8.4 (kernels RHCK y UEK)

macOS:

- 10.10 Yosemite macOS
- 10.11 el Capitan macOS
- 10.12 Sierra macOS
- 10.13 macOS High Sierra
- 10.14 MacOS Mojave
- 10.15 macOS Catalina
- macOS Big Sur 11.x (Intel)
- big sur macOS 11.x (M1)
- macOS Monterrey (Intel)
- macOS Monterrey (M1)

Android

- Lollipop 5.0/5.1
- Marshmallow 6.0
- Nougat 7.0 - 7.1
- Oreo 8.0
- Pie 9.0
- Android 10
- Android 11
- Android 12

iOS

- iOS 13 / iPadOS 13
- iOS 14 / iPadOS 14
- iOS 15 / iPadOS 15

5.4. PROTECCIÓN

La protección solicitada se dividirá en dos partes las cuales deberán combinarse e integrarse a nivel de configuración y se dividirán únicamente a nivel funcional. Deberá estar compuesto por solo un agente y una sola solución. No se permitirá el uso de diferentes componentes.

Plataforma de protección de endpoints (EPP)

Se requiere una solución de Endpoint Protection Platform (EPP) con las siguientes características:

- Antivirus para archivos, correo electrónico y web. Permitiendo la detección y desinfección de cualquier tipo de amenaza.
- Detección de malware e intentos de acceso a páginas web que contienen elementos maliciosos, bloqueándolos.
- Protección antimalware proactiva para estaciones de trabajo Windows, Linux y macOS.
- Protección antimalware proactiva para servidores Windows y Linux.
- Debe ser capaz de crear archivos "honeypot" para detectar ataques de ransomware basados en el comportamiento.
- Debería poder "congelar" el malware detectado durante siete días y, en caso de falso positivo, restaurar automáticamente el archivo afectado en el sistema.
- Debe tener tecnología de Deep Learning.
- Debe estar integrado con AMSI (AntiMalware Scan Interface).
- Firewall completo (IPv4 e IPv6), capaz de detectar automáticamente si los endpoints están conectados a una red pública o privada (reconocimiento de localización).
- Permitir la creación de reglas de firewall para redes públicas, redes privadas o ambas, debe permitir:
  - Conexiones entrantes y/o salientes bloqueadas de aplicaciones
  - Prevención de intrusiones - HIDS/HIPS
  - Crear una acción de reglas de firewall para permitir/denegar el tráfico entrante/saliente de las máquinas por protocolos/puertos.
  - Detección y bloqueo de intentos de explotación de vulnerabilidades mediante la supervisión del tráfico entrante
- Control de dispositivos, por categoría (unidades USB y módems, webcams, CD/DVD, Bluetooth, Escáneres, etc.) las acciones permitidas

de forma granular (acceso, bloqueo, lectura o grabación en su caso) para evitar la entrada de malware o fugas de datos. Por perfiles de configuración de protección y grupos de equipos.

- Control y seguimiento de la navegación web, filtrado por categorías, lista negra y lista blanca de URLs y pudiendo programar el funcionamiento de la regla (días de la semana x hora)
- Permite la detección de software no deseado y malware alojado en las aplicaciones en dispositivos Android.
- Proporcionará información sobre el hardware y el software instalados en los dispositivos Android.
- Protección proactiva para sistemas Android.
- Protección antirrobo para dispositivos Android (ubicación del equipo, posibilidad de tomar fotos después de 3 intentos fallidos de desbloqueo)
- Deshacer la funcionalidad de actualización si el dispositivo no tiene WIFI y no se analizará la inclusión de APK.
- Debe administrar de forma centralizada teléfonos inteligentes y tabletas con iOS 13 o superior para trabajar y navegar de forma segura.
- Debe tener un dispositivo antirrobo para dispositivos iOS con las siguientes características: geolocalización, limpieza remota, bloqueo remoto, foto del ladrón y alarma remota en caso de robo o pérdida del dispositivo.
- Debe tener filtrado URL para dispositivos iOS con la capacidad para denegar el acceso a las páginas pertenecientes a categorías en los días y horas seleccionados. Posibilidad de agregar URL a la lista blanca o lista de bloqueo.
- Debe tener protección web para dispositivos iOS que puedan filtrar URL maliciosas y de phishing.

Detección y respuesta de endpoints (EDR)

Se requiere una solución EDR (Detección y respuesta de endpoints) para protegerse contra las siguientes amenazas:

- Malware avanzado (conocido y desconocido)
- PUP (programas potencialmente no deseados)
- Amenazas de día cero
- Troyanos de nueva generación indetectables por antivirus.
- Esta solución tendrá que evitar infecciones tanto como sea posible de forma proactiva, nunca reactiva. La solución proporcionará contramedidas distintas de las siguientes:
  - Estructuras locales que requieren actualizaciones constantes.
  - Sistemas de lista blanca, que requiere personal dedicado para administrar este tipo de sistema.
  - Sistemas de análisis sandbox que consumen recursos, y que pueden ser eludidos por el malware.
- La solución deberá ser capaz de validar y clasificar todos los procesos ejecutados en las máquinas, clasificándolos como malware o goodware, para procesos desconocidos que requieren análisis manual (humano), la solución debe clasificar a través de sus laboratorios y con el menor tiempo posible desde el momento en que fueron interceptados en ejecución.

- Deberá bloquear los procesos desconocidos que intentan ejecutarse para evitar la posibilidad de dañar los datos accesibles a la máquina (como el cifrado no deseado) o el robo o acceso a los datos.
- Deberá ser posible establecer diferentes (más o menos restrictivos) y diferentes niveles de bloqueo en la capacidad de los usuarios para desbloquear individualmente los procesos bloqueados por el sistema.
- Debe detectar comportamientos extraños en motores de script como (Visual Basic Script, JavaScript y PowerShell) incrustados en todos los sistemas Windows actuales y macros maliciosas incrustadas en archivos de Office (Word, Excel, PowerPoint, etc.).
- Deberá poseer un modelo de "aprendizaje automático" con algoritmos basados en el modelo "ranker". Cada uno de ellos deberá estar diseñado para devolver el veredicto de calificación para cada proceso desconocido y host/usuario que intente ejecutarlo. Cada uno de ellos debe recibir una calificación, definida como una "puntuación". El veredicto final debe pesar sobre los resultados parciales elaborados con modelos de algoritmos predictivos y el modelo utilizado (conjunto) para garantizar la máxima precisión, certeza del resultado y un bajo número de falsos positivos.
- Deberá realizar clasificaciones de forma automatizada en un sistema de IA basado en la nube.
- Deberá detectar IOAs antes de que los datos se exfiltran (o cifren en caso de un ataque de ransomware) con un mecanismo de defensa, especialmente contra los ataques Living-off-the-Land (LotL), incluso si los puntos finales ya se han visto comprometidos.
- La solución deberá proporcionar análisis forense a los administradores con visibilidad de todas las acciones realizadas por el malware en las computadoras infectadas, así como información esencial para evaluar el nivel de riesgo de amenazas: vector de infección (cómo el malware ingresó a la red de la organización), patrón de propagación, si el malware accedió al disco duro de la computadora infectada para extraer información confidencial, y así sucesivamente.
- Deberá tener la línea de tiempo de los eventos y debe crearse automáticamente en función de los eventos de telemetría analizados. Los eventos de telemetría no deben considerarse incidentes, objetos malintencionados o anomalías en sí mismos. Deben representar la información vinculada a un objeto específico, por ejemplo:
  - Procesos: crear un proceso, ejecutar un proceso, inyectar un proceso en otro evento (hijo), etc.
  - Archivo: Creación de un nuevo archivo mediante un evento/proceso, edición de un archivo, eliminación de un archivo, apertura de un archivo, etc.
  - Comunicaciones: apertura de la comunicación, uso de un protocolo de comunicación, dirección de la comunicación, origen de la comunicación, etc.
  - Registro: creación, edición y eliminación de una clave de registro, etc.
  - Administración: uso de credenciales administrativas, eventos de inicio / cierre de sesión, instalación de procesos, actividad de servicio, etc.

- Capacidad de definir un área de software autorizado que se puede aplicar hash (MD5) u otros atributos de archivo (firma digital, nombre, ruta y versión), que se pueden combinar entre sí.
- Deberá incluir una caché local para evitar que el "goodware" se bloquee si la computadora protegida no puede conectarse a la plataforma en la nube.
- Debe contar con tecnologías para proteger los equipos de red de amenazas capaces de aprovechar las vulnerabilidades en el software instalado.
- Deberá contener ataques de fuerza bruta en el protocolo RDP.
- Deberá proteger contra vulnerabilidades conocidas y desconocidas (día cero).
- Deberá ser capaz de bloquear la Cadena de Eventos (CKC) de manera efectiva y en tiempo real, neutralizando los ataques de "exploits".
- Deberá detectar las técnicas de explotación de vulnerabilidades utilizadas por los hackers.
- Capaz de buscar patrones y detectar estáticamente de pares CVE-payload a través de archivos de firma.
- Deberá contar con tecnologías para proporcionar protección global anti-exploit contra técnicas avanzadas de exploit de vulnerabilidad
  - Ataque de reducción de superficie (ASR)
  - Prevención de ejecución de datos (DEP)
  - Protección contra sobreescritura de manejo de excepciones estructuradas (SEHOP)
  - Mitigación de seguridad de página nula
  - Asignación de pulverización de pila
  - Exportar filtrado de acceso a tablas de direcciones (EAF)
  - Aleatorización obligatoria del diseño del espacio de direcciones (ASLR)
  - Mitigación de seguridad ASLR de abajo hacia arriba
  - Comprobación de biblioteca de carga - Programación orientada a retornos (ROP)
  - Comprobación de protección de memoria - Programación orientada a retorno (ROP)
  - Comprobaciones de llamadas - Programación orientada a retornos (ROP)
  - Simular flujo de ejecución - Programación orientada al retorno (ROP)
  - Stack Pivot - Programación orientada al retorno (ROP)
  - EternalBlue
  - Proceso Doppelgänging
- Usted deberá analizar amenazas "sin archivos" / "sin malware".
- Deberá ser capaz de proteger contra las amenazas, que se ejecutan en la RAM de la computadora.
- La protección deberá ser capaz de prevenir los ataques mediante la supervisión continua de todos los procesos en ejecución y el análisis de su comportamiento.
- Deberá ser capaz de bloquear aplicaciones por hash o nombre del ejecutable.

- Deberá poder identificar los procesos que realizan una secuencia de acciones que se consideran peligrosas y se clasificarán como malware, independientemente de la cantidad de archivos que se coloquen en los medios de almacenamiento de la estación de trabajo o servidor de destino. Además, dado que todas las acciones realizadas por estos procesos deben registrarse en la nube, para realizar un análisis forense completo.
- Prestará un servicio de alerta y de medidas correctoras adecuadas cuando se detecte actividad anormal en el equipo en función del comportamiento normal previamente auditado en el parque de equipos.
- Este servicio debe ser ofrecido por el fabricante de la solución EDR por técnicos especializados, utilizando los datos recogidos en la auditoría forense.
- Debe ser capaz de implementar la alerta y la inclusión en la inteligencia del sistema EDR de medidas correctivas.
- Debe proporcionar un servicio de gestión que destaque lo que se puede identificar como un ataque de piratas informáticos, definido como un movimiento lateral que sigue a un ataque malicioso o comportamiento malicioso mediante el uso de software legítimo (sin la presencia de código malicioso).
- Debe ser capaz de advertir sobre los rastros de ataque o como resultado de un ataque en curso (IOA).
- La detección de la presencia de un atacante debe realizarse mediante:
  - Se descubrió un vector de ataque conocido en tiempo real (transmisión en tiempo real)
  - Se generó y validó la hipótesis de un ataque derivada de un comportamiento anómalo (IOA).
- Deberá tener una búsqueda proactiva y continua de ataques que aún son desconocidos y no identificables por las tecnologías de seguridad tradicionales.
- El servicio deberá buscar constantemente rastros y pistas de posibles ataques, generalmente aquellos que no son verificables por las tecnologías tradicionales de Endpoint Protection, para generar nuevas hipótesis verificables y crear nuevas reglas de detección.
- Las hipótesis generadas por este servicio de búsqueda continua y constante deben editarse, validarse y ejecutarse en la línea de tiempo de almacenamiento de eventos, recopilando todos los eventos de hosts protegidos en los últimos 12 meses.
- Cuando se valida una hipótesis formulada, el análisis deberá extenderse a la línea de tiempo de almacenamiento de eventos.
- El servicio deberá competir en la misma liga que los hackers y ciberdelincuentes más capaces de la actualidad.
- El servicio deberá estar totalmente gestionado y sin necesidad de un equipo interno que cuente con recursos especializados en ciberseguridad.

6. 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.

7. PLAZO DE ENTREGA

El plazo máximo de entrega es de 07 días calendarios, contados a partir del día siguiente de la firma del contrato, 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 General de Tecnologías de la Información.

8. FORMA DE ENTREGA

La entrega debe ser total, de acuerdo al plazo fijado.

9. 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 de la versión más reciente e 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.

10. 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.

11. CONFORMIDAD DE RECEPCIÓN DEL BIEN

La conformidad será emitida por cada responsable de oficina a través de un informe técnico de la Oficina de Informática.

12. PENALIDAD.

La penalidad se aplicará de acuerdo a la Ley de Contrataciones del Estado y su reglamento vigente.

GOBIERNO REGIONAL CUSCO
DIRECCIÓN REGIONAL DE EDUCACIÓN CUSCO
UNIDAD DE GESTIÓN EDUCATIVA LOCAL CUSCO

Bruno Gamarra Ortiz de Zevallos
RESPONSABLE 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 .....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 Nº 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

ANEXO N° 03

DECLARACION JURADA ANTISOBORNO

Yo, ... (Represéntate 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 o a lo establecido en el artículo 11 de la Ley de Contrataciones del Estado, Ley N° 30225, loa artículos 248° y 248° -A de su Reglamento aprobado mediante Decreto Supremo N° 350-2015-EF y sus modificatorias.

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 los artículos antes citados de la Ley de Contrataciones del Estado 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.

Cusco, ... de..... Del 2023

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