Fecha: 20-11-2025 Hora: 18:28:58

SOLICITUD DE COTIZACION Nro: 000629

UNIDAD EJECUTORA : 001 -Universidad Nacional De Arte Diego Quispe Tito Del Cusco
NRO. IDENTIFICACION : 001693

Razón Social:

Dirección: **R.U.C.**

Teléfono: **Fax:** **Pedido:** 000370

Concepto: ADQUISICION DE LICENCIA SOFTWARE ANTIVIRUS EMPRESARIAL

CANTIDAD REQUERIDA	UNIDAD MEDIDA	DESCRIPCION	PRECIO UNITARIO	PRECIO TOTAL
400.00	UNIDAD	SOFTWARE ANTIVIRUS		
			TOTAL	

Condiciones de compra y/o servicio:

Forma de pago:
Garantia:
Plazo de entrega en Nro Dias / Ejecución del servicio:
Tipo de moneda:
Validez de la cotización:
Indicar marca de procedencia:
Tipo de cambio:

Atentamente:

Firma y Sello Del Proveedor

DECLARACIÓN JURADA DE CUMPLIMIENTO DE TÉRMINOS DE REFERENCIA

Señores

UNIVERSIDAD NACIONAL DE ARTE DIEGO QUISPE TITO DE CUSCO
UNIDAD DE ABASTECIMIENTO

Presente. -

Es grato dirigirme a usted, para hacer de su conocimiento que luego de haber examinado los Términos de Referencia y demás documentos, conociendo todos los alcances y las condiciones detalladas en dichos documentos, el proveedor que suscribe ofrece el servicio de ...., cumpliendo con los requerimientos mínimos solicitados en el alcance del servicio de los Términos de Referencia.

Denominación o Razón Social:				Numero de RUC:	
Persona de contacto:			E-mail:		
Teléfono Fijo:		Celular:		Otros:	
NOTA: La omisión de alguno de los datos solicitados considera no válida la cotización.					

Cusco, ... de ..... del 2025

.....
Representante legal

ANEXO 7

DECLARACIÓN JURADA DE PARENTESCO Y NEPOTÍSMO

Yo,.....

Identificado (a) con D.N.I. N° ....., y domicilio actual en.....

DECLARO BAJO JURAMENTO:

NO	SI

Tengo parentesco hasta el cuarto grado de consanguinidad, segundo de afinidad, vínculo conyugal, de convivencia o unión de hecho con funcionarios o directivos de la UNADQTC.

En el caso de haber marcado como SI, señale lo siguiente.

Nombre completo de la persona con la que es pariente o tiene vínculo de afinidad, conyugal, de convivencia o unión de hecho, en la entidad.	
Cargo que ocupa	
El grado de parentesco	

Por lo que suscribo la presente en honor a la verdad.

Dado en la ciudad de..... a los.....días del mes de..... del 20.....

.....

(Firma)

DNI: .....

Huella digital
(índice derecho)

ANEXO 8

DECLARACIÓN JURADA DE DOBLE PERCEPCION EN EL ESTADO

Yo,
.....
identificado con DNI N° .....con dirección
domiciliaria:..... .....en el
Distrito: ..... Provincia: ..... Departamento.....

DECLARO BAJO JURAMENTO:

(NO) (SI) Tener conocimiento que ningún funcionario o servidor público puede desempeñar más de un empleo o cargo público remunerado, (*con excepción de uno más por función docente, de acuerdo a lo señalado en el numeral 13.2 de la norma técnica).

(NO) (SI) Percibir otra remuneración a cargo del Estado

En el caso de haber marcado como SI, señale lo siguiente.

Nombre de la Institución por la que percibe remuneración a cargo del Estado:	
Cargo que ocupa:	
Condición Laboral:	
Horario Laboral:	
Dirección de la institución:	

(NO) (SI) Tener incompatibilidad de distancia y con el horario de trabajo de dicho vínculo laboral.

Dado en la ciudad de..... a los.....días del mes de..... del 20.....

.....
Firma
DNI

Huella

*Art. 40° de la Constitución Política del Perú y artículo 3 de la Ley N° 28175 Ley Marco del Empleo Público.
La información contenida en la presente declaración jurada será sujeto de control posterior a cargo de la , a fin de corroborar la inexistencia de incompatibilidad horaria ni de distancia.

FORMATO DE CARTA DE AUTORIZACIÓN DE ABONO DIRECTO EN CUENTA (CCI)

CARTA DE AUTORIZACIÓN

Fecha:.....

Señores:
UNIVERSIDAD NACIONAL DIEGO QUISPE TITO

Asunto: Autorización de Abono directo en cuenta CCI que se detalla.

Por medio de la presente, comunico a usted, que la entidad bancaria, número de cuenta y el respectivo Código de Cuenta Interbancario (CCI) de la empresa que represento es la siguiente:

- Empresa (o nombre):.....
- RUC: .....
- Entidad Bancaria: .....
- Número de Cuenta: .....
- Código CCI: .....
- Cuenta de Detracción N°: .....

Dejo constancia que el número de cuenta bancaria que se comunica ESTÁ ASOCIADO al RUC consignado, tal como ha sido aperturada en el sistema bancario nacional.

Asimismo, dejo constancia que la (Factura o Recibo de Honorarios o Boleta de Venta) a ser emitida por mi representada, una vez cumplida o atendida la correspondiente Orden de Compra y/o Orden de Servicio con las prestaciones de bienes y/o servicios materia del contrato pertinente; quedará cancelada para todos sus efectos mediante la sola acreditación del abono en la entidad bancaria a que se refiere el primer párrafo de la presente.

Atentamente

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

ESPECIFICACIONES TÉCNICAS DEL REQUERIMIENTO

Unidad Orgánica	OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
Actividad del POI	FORMULACIÓN E IMPLEMENTACIÓN DEL SISTEMA INTEGRADO.
Denominación de la contratación	ADQUISICIÓN DE LICENCIAS SOFTWARE ANTIVIRUS EMPRESARIAL (CONSOLA DE ADMINISTRACIÓN CENTRALIZADA, ANTIVIRUS PARA COMPUTADORAS PERSONALES, ANTIVIRUS PARA LOS SERVIDORES DE APLICACIONES y/o DATOS) PARA ASEGURAR LA CONTINUIDAD OPERATIVA DE LA UNADQTC.
Meta presupuestaria	0012

1. Finalidad pública

La presente adquisición tiene como finalidad contribuir el cumplimiento del Reglamento de Organización y Funciones de la Oficina de Tecnologías de la Información. Los bienes permitirán que la Oficina de Tecnologías de la Información proporcione a la institución estas licencias de Software para el cumplimiento del ROF vigente y asegurar que los sistemas informáticos se mantengan protegidos y operativos, garantizando la disponibilidad, integridad de la información, así como la continuidad de los servicios brindados.

2. Objetivos de la contratación

- La Universidad Nacional De Arte Diego Quispe Tito del Cusco, requiere realizar la adquisición de las licencias antivirus, lo que permitirá a la UNADQTC contar con licencias permanentes de este software.
- Proteger contra malware: evitar la infección por virus, spyware, troyanos y otros tipos de malware que puedan comprometer la seguridad del sistema.
- Garantizar la seguridad en línea: proteger a los usuarios mientras navegan por internet, bloqueando sitios web maliciosos y phishing.

3. Alcances y Descripción de los Bienes a contratar

3.1. Descripción del Bien:

Ítem	Descripción	Cantidad	Unid. Medida
01	**ADQUISICIÓN DE LICENCIAS SOFTWARE ANTIVIRUS EMPRESARIAL (CONSOLA DE ADMINISTRACIÓN CENTRALIZADA, ANTIVIRUS PARA COMPUTADORAS PERSONALES, ANTIVIRUS PARA LOS SERVIDORES DE APLICACIONES y/o DATOS) PARA ASEGURAR LA CONTINUIDAD OPERATIVA DE LA UNADQTC.**	**400**	**Unidad**

3.2. Características Técnicas:

3.2.1. SOLUCIÓN DE PROTECCIÓN PARA ESTACIONES DE TRABAJO.

1) La solución deberá ser compatible con los siguientes sistemas operativos: Microsoft® Windows® 11/10(deben tener compatibilidad con la firma de código de Azure). Ubuntu Desktop 20.04 y superior x64, RedHat para Desktop 8, 9 x64 y superior, Linux Mint 21,22, Debian 12, Apple macOS 13 y superior.

2) El producto ofertado debe contar con un módulo de detección en tiempo real que proteja contra códigos maliciosos en cada ejecución, uso o creación de archivos en el equipo.

3) El producto ofertado debe contar con un sistema de detección de intrusos que realice un análisis de contenido del tráfico de red y además permita proteger de ataques haciendo que cualquier tráfico dañino sea bloqueado.

4) La solución es capaz de detectar todo tipo de amenazas, entre los más comunes: virus, gusanos, troyanos, spyware, adware, rootkits, bots, ransomware, etc.

5) La solución deberá contar con una funcionalidad de protección contra ransomware.

6) La solución ofertada deberá contar con un mecanismo de remediación de ransomware, capaz de realizar copias temporales de los archivos antes de que sean cifrados y restaurarlos en caso de ataque

7) Las copias temporales realizadas para la corrección deberán estar protegidas contra manipulación, borrado o cifrado por parte del propio malware.

8) Las copias temporales realizadas para la corrección deberán estar protegidas contra manipulación, borrado o cifrado por parte del propio malware.

9) El producto ofertado debe contar con la funcionalidad de evitar que el malware dañe o deshabilite la protección antivirus, por lo que se puede estar seguro de que el sistema permanece protegido constantemente.

10) La solución de protección de endpoints deberá integrarse nativamente con Intel® Threat Detection Technology (Intel® TDT), utilizando la telemetría de CPU para la detección de amenazas avanzadas, incluyendo ransomware, cryptojacking y malware fileless, optimizando el uso de recursos del endpoint mediante aceleración por hardware de Intel.

11) El programa antivirus debe contar con la opción de crear análisis bajo demanda. Estos análisis se podrán configurar para realizarse inmediatamente o a una fecha y hora futura, y también se podrán configurar para realizarse una vez o repetirse a diferentes intervalos, días, semanas, meses, etc.

12) Debe permitir elegir las unidades a escanear para los escaneos bajo demanda.

13) El producto ofertado debe ser capaz de crear exclusiones de escaneo ya sea por archivo, extensión o carpeta específica.

14) El producto ofertado debe pedir una contraseña ante intentos de cambio indebidos en la configuración del producto.

15) El cliente antivirus debe tener un agente que le permita ser administrado desde una consola centralizada. Este agente debe reportar el estado de todas las soluciones antivirus instaladas en la dependencia.

16) El producto ofertado deberá permitir generar dentro de la misma solución antivirus repositorios de actualización, los cuales deberán ser distribuidas mediante protocolo http localmente, sin depender de aplicaciones externas.
17) El producto ofertado debe tener una funcionalidad en donde todas las ventanas emergentes se deshabiliten y la protección del sistema seguirá ejecutándose en segundo plano, pero no requerirá ninguna interacción por parte del usuario.

18) El producto ofertado deberá tener una funcionalidad de catalogar a los procesos de los equipos de acuerdo con la reputación basada en la nube. Esta permitirá recopilar información anónima del ordenador afectada con las amenazas detectadas recientemente.

19) La solución debe tener sistema de prevención de intrusiones basado en el host, (HIPS).

20) El sistema HIPS debe tener los siguientes modos de configuración: automático, inteligente, interactivo, basado en políticas y aprendizaje.

21) El producto ofertado debe poseer un firewall bidireccional que contenga los siguientes modos de filtrado entre ellos, automático, interactivo, inteligente, aprendizaje y modo basado en políticas, además que pueda tener la capacidad de bloquear conexiones entrantes y salientes.

22) El 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.

23) El producto ofertado permitirá crear grupos que contengan varios vínculos URL para crear reglas de permiso y bloqueo a determinados sitios web.

24) El bloqueo web deberá poder asignarse por un rango de tiempo, por grupo y por equipo.

25) El producto ofertado debe tener un filtro antispam que permita integrarse con clientes de correo electrónico como Microsoft Outlook. Esta funcionalidad debe permitir al usuario generar una lista de direcciones de correos permitidas o bloqueadas.

26) El producto ofertado deberá analizar protocolos de e-mail POP3, IMAP.

27) La protección del correo electrónico en el cliente debe permitir definir si se desea escanear únicamente correo recibido, enviado o leído.

28) El producto ofertado debe tener la capacidad de añadir una nota o etiqueta en los correos electrónicos recibidos o leídos cuando se trate de mensajes no deseados o detectados.

29) La solución deberá contar con un módulo de protección Anti-Phishing que detecte sitios fraudulentos y bloquee el acceso total, evitando que los usuarios ingresen cualquier tipo de información.

30) El producto ofertado debe tener un módulo de protección para el acceso a la web para la detección y bloqueo de sitios web con contenido malicioso.

31) El producto ofertado debe ser capaz de escanear a través del protocolo SSL (HTTPS), de manera que se pueda impedir la descarga de archivos infectados.

32) El producto ofertado debe de permitir realizar exclusiones de URL para que no sean analizadas por el antivirus tanto en el protocolo HTTP, y HTTPS.

33) El producto ofertado debe tener un Módulo de control de dispositivos que permita acceso de solo lectura, lectura/escritura o bloquear dispositivos de acuerdo con una lista predefinida que incluya como mínimo: dispositivos USB, CD-ROM y dispositivos Bluetooth o módems.

34) El producto ofertado debe tener un módulo de control de dispositivos que permita crear varios grupos de dispositivos donde se podrán aplicar reglas distintas y además permitirá detectar los dispositivos conectados a la PC y agregarlos al listado de grupo de dispositivos. Además, incluye la capacidad de aplicar esta regla por un intervalo de horas y días específicos.
35) El producto debe contar con una primera exploración automática después de la instalación del programa, lo que permite asegurar que el equipo se encuentra protegido desde el comienzo.

36) El producto ofertado debe contar con una herramienta que permita examinar a fondo el ordenador, y con esta información poder ayudar a determinar la causa de un comportamiento sospechoso en el equipo que pueda deberse a una infección de malware o incompatibilidad de software o hardware. La información para recopilar deberá ser detallada sobre los componentes del sistema (como los controladores, aplicaciones instaladas, conexiones de red o entradas importantes del registro).

37) La solución deberá contar con la funcionalidad de bloqueo de exploits, que evite la explotación de vulnerabilidades en aplicaciones como los navegadores web, lectores de PDF, clientes por correos electrónicos y Microsoft Office componentes.

38) La solución deberá contar con un modo transparente de uso, en el cual no muestre ninguna alerta cuando se esté ejecutando una aplicación en pantalla completa.

39) La solución deberá contar con módulo de exploración avanzada de memoria que permita detectar las amenazas más sofisticadas que están diseñadas para evadir la detección a través de mecanismos tradicionales.

40) La solución de antivirus debe ejecutar un escaneo o exploración de cualquiera de los siguientes estados en la computadora (Protector de pantalla o salvapantallas activo, Sesión de usuario bloqueada, Sesión de usuario finalizada)

41) La solución deberá contar con un módulo de protección contra Botnets, este módulo debe ser capaz de detectar conexiones con servidores maliciosos de comando y control.

42) La solución deberá integrar un navegador seguro (Chrome), mostrando el logotipo de la solución presentada para asegurar que el módulo funcione correctamente, dando seguridad para proteger las transacciones bancarias, pagos en línea y sitios web.

43) La solución presentada incluirá una protección de la información ingresada con el teclado, contra registradores de pulsaciones al usar el navegador seguro.

3.2.2. SOLUCIÓN DE PROTECCIÓN PARA DISPOSITIVOS MOVILES

44) La solución deberá ser compatible con sistemas operativos Android 9 o superior.

45) La solución deberá proteger en tiempo real contra malware, escaneando automáticamente la carpeta descargas, los archivos de instalación APK y todos los archivos en la tarjeta SD una vez montada.

43) La solución deberá poder explorar de manera automática cuando el dispositivo está en estado inactivo (completamente cargado y conectado a un cargador).

44) La solución deberá contar con una exploración bajo demanda para la desinfección confiable de la memoria integrada y de los medios intercambiables.

45) La solución deberá contar con protección ante la desinstalación con una contraseña administrador.

46) La solución deberá tener una configuración de la seguridad de dispositivo con lo siguiente:

- Definir los requisitos sobre la complejidad de las contraseñas.
- Establecer una cantidad máxima de intentos de desbloqueo tras la cual el dispositivo entrará automáticamente en la configuración de fábrica.
- Establecer un vencimiento para el código de bloqueo de pantalla.
- Establecer un temporizador para el bloqueo de pantalla.
- Indicar a los usuarios que cifren el contenido de sus dispositivos móviles.
- Que notifique cuando se permita instalar de fuentes desconocidas.
- Que notifique cuando se haya desactivado el GPS.

47) La solución deberá permitir al administrador accionar los comandos remotos desde la consola mediante ejecución de tareas.

48) La solución deberá bloquear en forma remota los dispositivos perdidos o robados.

49) La solución deberá encontrar remotamente el teléfono y rastrear sus coordenadas de GPS.

50) La solución deberá eliminar en forma segura todos los contactos, los mensajes y los datos almacenados en la memoria interna del dispositivo, así como en las tarjetas de memoria SD.

51) La solución deberá poder activarse una alarma en el dispositivo que suene, incluso aunque el volumen esté en silencio.

52) La solución deberá poder hacer un restablecimiento remoto de la configuración predeterminada de fábrica.

53) La solución deberá poder monitorear las aplicaciones instaladas, bloquear el acceso a aplicaciones definidas y reducir el riesgo de exposición instando a los usuarios a desinstalar determinadas aplicaciones.

54) La solución deberá poder bloquear páginas web, aplicado mediante política de la consola administrativa.

55) La solución deberá poder recibir un mensaje personalizado por parte del administrador.

3.2.3. SOLUCIÓN DE PROTECCIÓN PARA SERVIDORES

Se debe considerar licencias de Antivirus, para todos los servidores, con las siguientes características:

56) La solución debe ser compatible con los siguientes sistemas operativos: Windows Server
2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows
Server 2025 cuales deben tener compatibilidad con la firma de código de Azure.

57) El producto antivirus puede instalarse sobre plataformas de x64 bits RedHat Enterprise Linux (RHEL) 8 ,9 y 10; Ubuntu Server 22.04 y 24.04 LTS; Debian11 y 12; SUSE Linux Enterprise Server (SLES) 15, Rocky Linux 8,9 y 10.

58) Compatible con versiones del kernel del sistema operativo Linux 4.18 y posteriores

59) El producto 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)

60) La solución es capaz de detectar todo tipo de amenazas, entre los más comunes: virus, gusanos, troyanos, spyware, adware, rootkits, bots, ransomware, etc.

61) La solución deberá contar con una funcionalidad antiransomware.

62) El producto 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.

63) El producto 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.

64) El producto debe ser capaz de crear exclusiones de escaneo ya sea por archivo, extensión o carpeta específica.

65) El producto debe pedir una contraseña ante intentos de cambio indebidos en la configuración del producto.

66) El producto debe contar con un agente que le permita ser administrado desde una consola centralizada.

67) El antivirus deberá 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.

68) La protección en tiempo real debe iniciarse con el sistema operativo, así como poder definir qué tipos de medios serán analizados por el módulo.

69) La solución debe tener sistema de prevención de intrusiones basado en el host, (HIPS).

70) El sistema HIPS debe tener los siguientes modos de configuración: automático, inteligente, interactivo, basado en políticas y aprendizaje.

71) El producto debe permitir escanear archivos comprimidos.

72) Debe permitir elegir las unidades a escanear para los escaneos bajo demanda.

73) En sistemas operativos Windows, el antivirus 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.

3.2.4. SANDBOXING.

74) Uso de Sandboxing en la nube para analizar el comportamiento de archivos, con tiempo máximo de espera por el resultado del análisis de 5 minutos.

75) Es posible crear una exclusión por ruta, detección y su hash (SHA-1).

76) Capacidad de sincronizar su licenciamiento con la nube y la consola de administración en sitio o en la nube.

77) 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.

78) Debe borrar automáticamente las muestras de los archivos/ejecutables en los servidores donde fue analizado el comportamiento.

79) Capacidad para enviar correos SPAM para su análisis.

80) Debe tener únicamente estos umbrales de detección: desconocido, limpio, sospechoso, altamente sospechoso y malicioso.

81) 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.

82) Debe tener protección proactiva, es decir, que el archivo/ejecutable sea bloqueado hasta recibir el resultado del Sandbox en la nube.

83) Se debe tener capacidad para integrarse con la solución de antimalware o protección del punto final, para tener mayores posibilidades de protección y aplicación de políticas.

84) Enviar un archivo/ejecutable a través de una consola de administración del punto final.

3.2.5. CIFRADO DE DISCO.

85) La solución deberá compatible con sistemas Windows 10 y 11(64bits).

86) La solución es compatible en discos con esquema de particiones GPT.

87) La solución es compatible con UEFI.

88) La solución deberá ser capaz de cifrar los Endpoints seleccionados desde el inicio de sistema.

89) La solución deberá disponer de diversas posibilidades de recuperación de Passwords para usuarios remotos que se vean bloqueados.

90) La solución deberá poder programar las tareas de cifrado sobre los Endpoints seleccionados con la posibilidad de pausar la ejecución para retomar luego desde el último punto.

91) La solución deberá poder ser administrada desde la misma consola central junto con las otras soluciones descriptas en el TDR.

3.2.6. CONSOLA DE ADMINISTRACIÓN CENTRALIZADA.

92) La consola debe ser con infraestructura en la nube, implementado como un servicio SAAS, adicionalmente debe tener la capacidad de implementarse en forma On-premise.

93) La consola de administración debe permitir la configuración y administración remota de la solución antivirus instalada en los puntos finales (Windows, Linux, Mac, Android).

94) 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.

95) 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.
96) 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.

97) La consola de acceso al servidor deberá ser 100% web, siendo compatible con los siguientes navegadores: Mozilla Firefox, Microsoft Edge, Google Chrome, Safari, Opera.

98) 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.

99) 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.

100) El producto debe ser capaz de mostrar los equipos detectados en la red.

101) La consola de administración centralizada debe tener la capacidad de mostrar los intentos de infección de virus en los equipos clientes.

102) El producto debe ser capaz de controlar a través de políticas todos los componentes mencionados anteriormente (para Workstation y servers) sin necesidad de consolas adicionales para la creación de políticas.

103) El producto debe poseer una interfaz web que permita monitorear el estado de los equipos en la red, así como también, mostrar como mínimo reportes sobre: clientes con mayor registro de amenazas, principales amenazas, clientes con más amenazas, clientes actualizados /no actualizados y sistemas operativos administrados.

104) El producto debe permitir la instalación y desinstalación remota de la solución de seguridad con opción a desinstalar antivirus de terceros.

105) El producto debe permitir la generación de reportes gráficos y personalización de estos.

106) Los reportes deben ser fácilmente exportables en formatos CSV, PDF.

107) El producto debe contar con una herramienta 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.

108) El producto debe ser capaz de generación de alertas ante un evento específico mediante el envío de un correo.

109) Las actualizaciones deben ser descargadas directamente desde los servidores del fabricante y con la opción de usar repositorio instalado en un servidor compatible para que los clientes actualicen desde sus definiciones de virus, phishing, spam, bases de datos de URLs maliciosas, actualización de parches del producto entre otras.

110) 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.

111) La solución debe permitir el manejo flexible de las licencias, de manera que puedan ser reasignadas en caso se restaure el sistema o se cambie de equipo.

112) Deberá permitir la ejecución remota de scripts, batch files y paquetes personalizados de terceros a través de la consola.

113) Deberá permitir generar grupos de clientes dinámicos y grupos estáticos.

3.2.7. 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) Que tenga oficinas de la marca en Latinoamérica y presencia local en el país.

3.3. INSTALACIÓN Y CONFIGURACIÓN:

- El CONTRATISTA, antes de proceder a la instalación deberá convocar a una reunión de Kick-Off del proyecto para presentar un plan de trabajo (implementación de la solución), así como la arquitectura planteada que se ajuste a las especificaciones técnicas y topología de la red de la UNADQTC.
- El CONTRATISTA deberá configurar las políticas, previamente coordinadas con la UNADQTC.
- Se debe considerar que los trabajos que impliquen la interrupción de las actividades de los usuarios de la UNADQTC, deberán ser realizados los días laborables a partir de las 17:00 horas o en su defecto los fines de semana, previa coordinación con la OTI de la UNADQTC.
- En la etapa de pruebas, en caso exista falsos positivos, se deber reconfigurar la solución propuesta, hasta que se llegue a minimizar los mismos.
- La implementación de la solución deberá realizarse en **tres (03) días calendario** contados a partir del día siguiente de la entrega del bien.

3.4. TRANSFERENCIA DE CONOCIMIENTO.

El contratista deberá brindar una transferencia de conocimiento virtual o presencial para el personal de la **OTI**, el cual debe ser de un total de **cuatro (04) horas**, sobre la arquitectura y administración de la solución, debiendo entregar constancias y/o actas de participación a los asistentes.

La coordinación referente al horario y lugar de la capacitación deberán ser coordinadas con la OTI, a través de correo electrónico y/o coordinaciones telefónicas.

La capacitación deberá contener los siguientes temas:

- Instalación
- Configuración
- Administración
- Solución de problemas sabre los componentes de la herramienta
- Durante el curso de capacitación el oferente deberá realizar pruebas de ataques
- reales, infectando una máquina de prueba
- Despliegue de políticas de seguridad de la consola instalada en la red de la UNADQTC.

El expositor deberá ser un personal certificado por el fabricante, el cual deberá contar por lo menos con una experiencia de dos (02) años capacitando en el uso y administración de la herramienta de Software Antivirus ofertada.

Al finalizar la capacitación para el personal **OTI**, el contratista deberá otorgar certificados de Operador y Administrador de Consola del producto adquirido a los participantes.

3.5. SOPORTE TÉCNICO

a) Soporte técnico y vigencia de las licencias de Software antivirus por ***tres (03) años*** *ó* **treinta y seis (36) meses**.

b) Se acompañará al personal administrativo de la institución con asesorías el tiempo que dure la garantía (según numeral 4).

c) El contratista debe contar con soporte técnico 24x7x365 con la posibilidad de escalar casos técnicos en cualquier momento hacia la casa matriz haciendo uso del sistema del fabricante.

3.6. ENTREGABLES

a) El software de licencias antivirus deberá ser registrado a nombre de la UNADQTC. El contratista deberá entregar el documento donde se especifique las cuatrocientas (400) licencias de antivirus con su soporte respectivo, así como con una vigencia de ***tres (03) años*** *ó* **36 meses**.

b) Informe de instalación y puesta en funcionamiento del Software Antivirus.

c) Procedimiento de escalamiento de fallas, así como datos de los contactos de soporte técnico.

d) Certificados de Capacitación (versión física o digital) otorgados por el Contratista y/o marca.

4. GARANTÍA

- El contratista brindara una garantía de **1095 días** calendario o **36 meses** para la solución y vigencia de la suscripción del licenciamiento.

5. REQUISITOS DEL PROVEEDOR Y/O PERSONAL

- Ser persona natural o jurídica, tener RUC activo y vigente y estar habilitado para contratar con el Estado y tener RNP.
- Tener Registro Único de Contribuyente habilitado y a fin del rubro a contratar.
- No estar sancionados y/o inhabilitado para contratar con el estado.

Experiencia Personal Clave:

- **Jefe De Proyecto (01 Profesional)**

  Formación Académica

  Profesional titulado, colegiado y habilitado en Ingeniería Informática, Ingeniería de Software, Ingeniería de Sistemas o carreras afines.

  La formación se acreditará mediante copia del título profesional y constancia de habilitación vigente.

  Experiencia General

  Mínimo 5 años de experiencia en instituciones públicas y/o privadas desempeñando funciones como responsable, administrador o encargado de centros de cómputo, o en roles relacionados al desarrollo, análisis de sistemas (software) o consultorías informáticas.

  Experiencia Específica

  Mínimo 2 años de experiencia específica en desarrollo de software en servicios, consultorías o como profesional de planta.

  Cursos y Capacitaciones

  - Curso en administración de servidores Linux.
  - Cursos en metodologías ágiles: PMI y/o PMP y/o SCRUM.
  - Curso de seguridad informática orientada a empresas.

- **Especialista (01 Profesional)**

  Formación Académica

  Profesional titulado en Ingeniería Informática, Ingeniería de Software, Ingeniería de Sistemas o carreras afines.

  La formación se acreditará mediante copia del título profesional y constancia de habilitación vigente.

  Experiencia General

  Mínimo 2 años de experiencia en servicios informáticos, consultorías o como profesional de planta.

  Experiencia Específica

  Mínimo 2 años de experiencia específica en desarrollo de software en servicios, consultorías o como profesional de planta.

  Cursos y Capacitaciones

  - Curso en terminal y línea de comandos (mínimo 10 horas).
  - Certificación en tecnologías de software Microsoft.
  - Certificación en tecnologías de software de protección para ordenadores y/o servidores.
  - Curso en Docker (mínimo 20 horas).
  - Cursos en gestión de proyectos (mínimo 15 horas).

- La acreditación será mediante copias simples de actas de conformidad, orden de servicio, orden de compras y comprobantes de pagos, constancias, certificados.

6. Lugar y Plazo de Ejecución

Lugar:

- La entrega de la Suscripción del licenciamiento del software de antivirus a nombre de la UNADQTC en formato físico, en hoja membretada y en sobre lacrado, en el Almacén Central de la Universidad Nacional de Arte Diego Quispe Tito del Cusco. Av. Huayruropata 1602.
- La instalación, implementación y puesta en operación del bien solicitado se realizar en el Centro de Datos de la entidad.

Plazo:

a. El plazo de entrega es de **dos (2) días calendario**, contabilizado a partir del día siguiente de la notificación de la orden de compra.

b. La implementación de la solución deber realizarse hasta **tres (3) días calendario** contados a partir del día siguiente de la entrega de la suscripción del licenciamiento. La Implementación, configuración y funcionamiento debe constar como mínimo de las siguientes actividades:

- Los trabajos programados serán supervisados por el jefe de la OTI de la UNADQTC.
- Toda la solución debe estar basada únicamente en software, la solución no deberá incluir la adquisición de ningún tipo de equipamiento adicional como complemento de este.
- El software no debe afectar lentitud en los equipos de cómputo conectados a la Red de la UNADQTC.
- El postor deberá proporcionar las herramientas, accesorios y personal técnico necesarios para llevar a cabo la instalación del software antivirus.
- Transferencia del Conocimiento.

7. Conformidad

La conformidad estará a cargo de la Oficina de Tecnologías de la Información, quien verificará el cumplimiento del servicio de acuerdo a lo solicitado en los presentes Términos de Referencia, en concordancia con el artículo 168 del Reglamento de la Ley de Contrataciones del Estado.

8. Forma y Condiciones de Pago

El pago se efectuará en una (1) armada, en moneda nacional, previa conformidad del área usuaria, presentación de carta mediante mesa de partes indicando el cumplimiento de la adquisición, Manuales de usuario y del sistema, y verificación del sistema.

9. Penalidades

Penalidad por Mora en la ejecución de la prestación:
En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso. La penalidad se aplica automáticamente y se calcula de acuerdo a la siguiente fórmula:

$$\text{Penalidad diaria} = \frac{0.10 \; x \; monto}{F \; x \; plazo \; en \; días}$$

Donde F tiene los siguientes valores:

a) Para plazos menores o iguales a sesenta (60) días, para bienes, servicios en general, consultorías en general y ejecución de obras: F = 0.40.
b) Para plazos mayores a sesenta (60) días:
   b.1) Para bienes, servicios y consultorías en general: F = 0.25.
   b.2) Para obras: F = 0.15.

Tanto el monto como el plazo se refieren, según corresponda, a la ejecución total del servicio o a la obligación parcial, de ser el caso, que fuera materia de retraso.

Se considera justificado el retraso, cuando el contratista acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable.

Esta calificación del retraso como justificado no da lugar al pago de gastos generales de ningún tipo.

10. Responsabilidad por vicios ocultos

El contratista es el responsable por la calidad ofrecida y por los vicios ocultos de los bienes y servicios conexos. Asimismo, ser responsable por los daños y perjuicios originados al contratante, como consecuencia del incumplimiento de lo ofertado y de la prestación deficiente del bien y/o servicio. El plazo mínimo de responsabilidad ser de treinta y seis (36) meses contabilizados a partir del día siguiente de otorgada la conformidad. La Oficina de Tecnologías de la Información o quien asuma sus funciones, no enerva su derecho de reclamar posteriormente por defectos o vicios ocultos.

11. Propiedad intelectual y confidencialidad

La Entidad tendrá todos los derechos de propiedad intelectual incluidos, sin limitación, así como las patentes, derechos de autor, nombres comerciales y marcas registradas respecto a los productos o documentos y otros materiales que guarden una relación directa con la ejecución del servicio o que se hubiere creado o producido como consecuencia o en el desarrollo de la ejecución del servicio. Asimismo, el contratista se obliga a mantener y guardar estricta reserva y absoluta confidencialidad de todos los documentos e informaciones de la Entidad, a los que tenga acceso con motivo del desarrollo del presente servicio. Dicha obligación comprende la información que se entrega, como también la que se genera durante la realización de toda actividad e información producida una vez que se haya concluido el servicio. Dicha información puede consistir en fotografías, informes, material videográfico, documentos y otros similares.

12. Clausula anticorrupción

EL PROVEEDOR declara y garantiza no haber, directa o indirectamente, o tratándose de una persona 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 el 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.

Asimismo, El PROVEEDOR 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, participacioncitas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado.

Además, EL PROVEEDOR se compromete a:

i) Comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y
ii) Adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas.

Finalmente, sírvase verificar la Política y Objetivos de Gestión Antisoborno de la CGR, en la siguiente ruta web:

https://busquedas.elperuano.pe/normaslegales/aprueban-la-politica-y-objetivosde-gestion-antisoborno-de-l-resolucion-no-092-2021-cg-1939721-1/

13. *Solución de Controversias*

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante **conciliación**, según el numeral 81.3 del artículo 81 de la Ley N°32069, Ley General de Contrataciones Públicas.

Cualquiera de las partes tiene el derecho a solicitar una conciliación dentro del plazo de caducidad correspondiente, según lo señalado en el artículo 82 de la Ley N° 32069, Ley General de Contrataciones Públicas, sin perjuicio de recurrir al arbitraje, en caso no se llegue a un acuerdo entre ambas partes o se llegue a un acuerdo parcial. Las controversias sobre nulidad del contrato solo pueden ser sometidas a arbitraje.

14. *Resolución de contrato por incumplimiento*

Cualquiera de las partes puede resolver el contrato, de conformidad con el literal b) del numeral 68.1 del artículo 68 de la Ley N° 32069, Ley General de Contrataciones Públicas "*Incumplimiento de obligaciones contractuales, por causa atribuible a la parte que incumple*". Siendo el procedimiento que seguir lo establecido en el artículo 122 del Reglamento de la Ley N°32069, Ley General de Contrataciones Públicas.

15. *Gestión de riesgo*

El Contratista y la Entidad, toman conocimiento aprovechando el impacto de riesgos positivos y disminuyendo la probabilidad de los riesgos negativos y su impacto durante la ejecución contractual, considerando la finalidad pública de la contratación.

UNIVERSIDAD NACIONAL DE ARTE DIEGO QUISPE TITO DEL CUSCO

Ing. Edson Gary Vasquez Chellco

Firma del Responsable de la Unidad Orgánica

Fecha: 20-11-2025 Hora: 18:28:58

SOLICITUD DE COTIZACION Nro: 000629

UNIDAD EJECUTORA : 001 -Universidad Nacional De Arte Diego Quispe Tito Del Cusco
NRO. IDENTIFICACION : 001693

Razón Social:

Dirección: **R.U.C.**

Teléfono: **Fax:** **Pedido:** 000370

Concepto: ADQUISICION DE LICENCIA SOFTWARE ANTIVIRUS EMPRESARIAL

CANTIDAD REQUERIDA	UNIDAD MEDIDA	DESCRIPCION	PRECIO UNITARIO	PRECIO TOTAL
400.00	UNIDAD	SOFTWARE ANTIVIRUS		
			TOTAL	

Condiciones de compra y/o servicio:

Forma de pago:
Garantia:
Plazo de entrega en Nro Dias / Ejecución del servicio:
Tipo de moneda:
Validez de la cotización:
Indicar marca de procedencia:
Tipo de cambio:

Atentamente:

Firma y Sello Del Proveedor