ESPECIFICACIONES TECNICAS PARA LA ADQUISICIÓN DE LICENCIAS DE SOFTWARE ANTIVIRUS.

1. ÁREA QUE REALIZA EL REQUERIMIENTO.

Área de Tecnologías de la Información y Telecomunicaciones del Hospital Regional del Cusco.

2. OBJETO DE LA CONTRATACIÓN|.

Adquirir Licencias de Software Antivirus que permita la protección de la información almacenada en las Computadoras personales y Sistemas Informáticos pertenecientes al Hospital Regional del Cusco.

3. FINALIDAD PÚBLICA

El presente proceso permitirá continuar las condiciones de seguridad de los usuarios que usan los equipos de cómputo de la entidad, a fin de cumplir con las funciones asignadas de conformidad con lo regulado en el Reglamento de la Organización y Funciones - ROF de la Entidad.

4. OBJETIVOS DE LA CONTRATACIÓN.

4.1 Objetivo General

Garantizar la disponibilidad en integridad de la Información contenida en las Computadoras personales, así como en los Sistemas Informáticos del Hospital Regional Cusco a fin de garantizar su disponibilidad y confiabilidad.

5. DESCRIPCIÓN DE LOS BIENES.

ITEM	DESCRIPCIÓN	CANTIDAD	UNIDAD DE MEDIDA
01	Adquisición de licencias de Software Antivirus empresarial (Consola de administración centralizada, Antivirus para Computadoras personales, Antivirus para los Servidores de aplicaciones y/o Datos).	250	Unidad

5.1 Cantidad de Licenciamiento de Software de Antivirus.

Como parte del Servicio de Implementación de Software de Antivirus se requiere adquirir doscientos cincuenta (250) licencias de software antivirus compatibles con los siguientes Sistemas Operativos:

Sistemas operativos de estaciones de trabajo (en versiones de 32/64 bits).

a) Microsoft Windows 10
b) Microsoft Windows 7 SP 1
c) Microsoft Windows 8 (8.1).

Sistemas operativos de servidores de red (en versiones de 32/64 bits).

a) Microsoft Windows 2008 R2 Server.
b) Microsoft Windows 2012 R2 Server.

5.2 Características Técnicas del Software Antivirus.

La entidad solicita la adquisición de software antivirus de un solo fabricante, el cual deberá contener una consola de administración centralizada, así como un agente que cubra con los requerimientos técnicos mínimos indicados a continuación:

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 20, 21,22 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 debe contar con una funcionalidad de corrección de ransomware que realice copias de seguridad y restaure archivos dañados, dicho proceso se activa cuando la detección del ransomware se ha realizado previamente.

7) 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.

8) 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.

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

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

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

12) 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.

13) 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.

14) 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.

15) 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.

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

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

18) 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.

19) 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.

20) El 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 deberá poder asignarse por un rango de tiempo, por grupo y por equipo.

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

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

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

25) 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.

26) 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.

27) 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.

28) 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.

29) 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.

30) 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.

31) El producto ofertado debe tener un módulo de control de dispositivos que permita crear varios grupos de dispositivos donde se podrán aplicar reglas distintas y además permitirá detectar los dispositivos conectados a la PC y agregarlos al listado de grupo de dispositivos. Además, incluye la funcionalidad de aplicar esta regla por un período de tiempo determinado (hora y días).

32) 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.

33) 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).

34) 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.

35) 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.

36) 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.

37) 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)

38) 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.

39) 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.

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

3.- SOLUCIÓN DE PROTECCIÓN PARA SERVIDORES

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

41) La solución debe ser compatible con los siguientes sistemas operativos: Windows 2008 Server R2, 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.

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

43) Compatible con versiones del kernel del sistema operativo Linux 4.14 y posteriores

44) 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)

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

46) La solución deberá contar con una funcionalidad antiransomware.

47) 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.

48) 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.

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

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

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

52) 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.

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

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

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

56) El producto debe permitir escanear archivos comprimidos.

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

58) 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.

4. SANDBOXING.

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

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

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

76) 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.

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

78) Capacidad para enviar correos SPAM para su análisis.

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

80) 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.

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

82) 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.

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

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 deseados 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 deseados 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.

6. DETECCION Y RESPUESTA EXTENDIDA:

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

93) El agente de la solución deberá ser compatible con los siguientes sistemas operativos:

- Microsoft® Windows® 11/10(deben tener compatibilidad con la firma de código de Azure).
- Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022(cuales deben tener compatibilidad con la firma de código de Azure).
- Linux de x64 bits: RedHat Enterprise Linux (RHEL) 8 y 9; Ubuntu Server 22.04 y
  24.04 LTS; Debian11 y 12; SUSE Linux Enterprise Server (SLES) 15.
- MacOS 13 o superior.

94) La herramienta debe suministrar prevención contra amenazas, visibilidad y respuesta ante incidentes
95) Debe permitir identificar comportamientos anómalos dentro de la red
96) La herramienta debe facilitar información para poder hacer investigaciones y tomar medidas correctivas.
97) Debe poder identificar indicadores de compromisos.
98) Debe permitir configurar filtros múltiples para poder detectar amenazas con facilidad.
99) Debe poder realizar acciones de respuestas con un solo click.
100) Debe contar con acceso remoto.
101) La herramienta debe permitir aislar equipos de la red para detener movimientos laterales
102) La herramienta debe proporcionar la visibilidad total y poder realizar el análisis de la causa de origen del posible ataque, mostrando el árbol de procesos completos para cualquier cadena de eventos potencialmente maliciosos.
103) La herramienta debe tener acceso a información del Framework de Mitre Attack
104) La herramienta debe tener integración con la información mostrada en Virus Total
105) La herramienta debe poder mostrar la reputación de las acciones llevadas por algún ejecutable
106) La herramienta debe contar con reglas predefinidas agrupadas por categorías.
107) La herramienta debe permitir crear propias reglas de monitoreo.
108) La herramienta debe contar con una API pública que permita integrar con herramientas SIEM, SOAR y sistemas de tickets.

109) La herramienta debe permitir visualizar y bloquear módulos en función de más de 30 indicadores diferentes, incluyendo el valor de hash, las modificaciones del registro, las modificaciones de archivos y las conexiones de red.
110) Debe permitir agregar o quitar etiquetas para filtrar más rápido los objetos, como computadoras, alarmas, exclusiones, tareas, ejecutables, procesos y scripts.
111) Debe permitir priorizar la severidad de las alarmas mediante la funcionalidad de puntaje, que atribuya un valor de gravedad a los eventos y permita a los administradores identificar fácilmente las computadoras que corren mayor riesgo de sufrir un incidente potencial.
112) La herramienta debe bloquear la ejecución de módulos maliciosos en todas las computadoras de su red corporativa.
113) La herramienta debe visibilizar la información detallada de los módulos recién ejecutados, incluyendo el tiempo de ejecución, el usuario que lo ejecutó, el tiempo de espera y los dispositivos atacados.
114) La herramienta debe permitir bloquear la ejecución de scripts o aplicaciones no autorizados.
115) La herramienta debe contar con machine learning y acciones automatizadas.
116) La herramienta debe poder entender el comportamiento de los equipos y mostrar las alarmas comunes para su filtrado.

7. CONSOLA DE ADMINISTRACIÓN CENTRALIZADA.

117) 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.

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

119) 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.

120) 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.

121) 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.

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

123) 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.

124) 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.

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

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

127) 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.

128) 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.

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

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

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

132) 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.

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

134) 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.

135) 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.

136) 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.

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

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

8. OTROS:

a. El fabricante deberá tener soporte técnico en español 24 X 7 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.

c. Debe permitir realizar una instalación remota.

d. Debe permitir desinstalar otros productos antivirus remotamente al lanzar la instalación.

e. Debe permitir realizar exclusiones de análisis por hash, proceso y extensión como mínimo.

f. Proporcionar, con el correspondiente respaldo del fabricante, el mantenimiento de software, por el período de las licencias.

g. Las actualizaciones del Centro de Control en la nube deben ser automáticas sin requerir la intervención del administrador.

6.3 Actividades:

La implementación, configuración y funcionamiento del producto adquirido deberá cumplir las siguientes condiciones:

- Los trabajos programados serán supervisados por el personal del Área de Tecnologías de Información y Telecomunicaciones del Hospital Regional del Cusco.
- Instalación de la herramienta para el Hospital Regional del Cusco.
- Instalación y configuración de la consola web para las doscientos cincuenta (250) **estaciones** de trabajo, ubicados en la sede del Hospital Regional del Cusco, los cuales podrán ser visualizadas en la consola principal. Asimismo, deberán contar con las respectivas pruebas de actualización de firmas, versión del cliente, cambio de configuración entre otros.
- 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 del Hospital Regional Cusco.
- El postor deberá asegurar la desinstalación de la versión actual en las estaciones de trabajo desde la consola de administración o mediante script de desinstalación sin afectar las labores de los usuarios finales.
- El postor deberá proporcionar personal técnico en caso la desinstalación no se pueda realizar por consola y se tenga que hacer de manera manual.
- El postor deberá proporcionar las herramientas, accesorios y personal técnico necesarios para llevar a cabo la instalación del software antivirus.

6.4 Capacitación

El contratista deberá brindar una capacitación virtual o presencial para el personal técnico del Área de Tecnologías de la Información y Telecomunicaciones (ATIT), la cual debe ser de un total de cuatro (04) horas y para seis (06) personas como mínimo.

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

GOBIERNO REGIONAL CUSCO HOSPITAL REGIONAL CUSCO DIRECCIÓN REGIONAL DE SALUD CUSCO

05

La capacitación deberá contener los siguientes temas:

- Instalación
- Configuración
- Administración
- Solución de problemas sobre 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 del Hospital Regional Cusco.

El desarrollo de la capacitación incluirá archivos digitales, separatas, manuales y videos para el dictado del curso, los cuales deberán ser referidos a la configuración, instalación y administración de la consola del producto adquirido.

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 técnico que el Área de Tecnologías de la Información y Telecomunicaciones (ATIT) designe, el contratista deberá otorgar certificados de Operador y Administrador de Consola del producto adquirido a los participantes.

6.5 Soporte Técnico

a) Soporte técnico y vigencia de las licencias de Software antivirus por doce (12) meses.

b) 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.

6.6 Resultados Esperados

Entregables:

a) El software de licencias antivirus deberá ser registrado a nombre del Hospital Regional del Cusco. El contratista deberá entregar el documento donde se especifique las doscientos cincuenta () licencias de antivirus con su soporte respectivo, así como con una vigencia de un (01) año.
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, incluyendo separatas y manuales de usuario.

6.8 Otras consideraciones para la ejecución de la prestación:

a) A fin de poder elaborar su mejor propuesta, el contratista podrá realizar una visita a la Oficina de Tecnología de Información (OTI) y solicitar la información pertinente, durante los horarios de oficina (8:30 am – 5:30 pm), a fin de obtener un mejor conocimiento de la implementación, equipamiento técnico, necesidades de

configuración de los equipos u otros componentes, que tengan que incluir en la implementación y ejecución del requerimiento.

b) El software de antivirus provisto por el contratista debe cumplir con las características técnicas solicitadas.
c) En la implementación, el contratista deberá trabajar de manera conjunta con el personal técnico de la Oficina de Tecnología de Información asignado para la instalación y puesta en operación del bien.
d) Las pruebas que se requieran no deberán afectar las labores y la red del HRC.
e) El Contratista junto con el personal de la Oficina de Tecnología de Información, deberán realizar las pruebas o ensayos que serán de uso para la conformidad de los entregables, con el fin de dar cumplimiento a las especificaciones técnicas.
f) El Contratista deberá cumplir con las políticas de seguridad y con los procedimientos y políticas para el manejo de los recursos tecnológicos definidos por el HRC.

7. PLAZO DE ENTREGA

Hasta diez (07) días calendarios contabilizados desde el día siguiente de emitida la orden de compra.

8. LUGAR DE ENTREGA E INSTALACIÓN

La entrega se realizará en el almacén del Hospital Regional del Cusco, sito Av. La Cultura S/N, Cusco, en el horario de 08:00 a 15:00 hrs.

La instalación, implementación y puesta en operación del bien solicitado se realizará en el Centro de Datos de la entidad.

9. CONFORMIDAD

La conformidad del bien será entregada por el Área de Tecnología de Información y Telecomunicaciones, previo cumplimiento de lo solicitado en el punto 6 de los términos de referencia.

10. FORMA Y CONDICIONES DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en PAGO UNICO

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- Conformidad otorgada por el área usuaria.
- Comprobante de pago.

La Entidad debe pagar las contraprestaciones pactadas a favor del contratista dentro de los diez (10) días calendario siguiente a la conformidad de los bienes, siempre que se verifiquen las condiciones establecidas en el contrato.

11. RESPONSABILIDAD DEL CONTRATISTA

El contratista es el responsable por la calidad ofrecida y por los vicios ocultos del bien ofertado por un plazo no menor de un (01) año, contado a partir de la conformidad otorgada por la Entidad.

12. 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:

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

Donde F = 0.40.

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.

13. RESOLUCIÓN CONTRACTUAL

El Hospital Regional Cusco puede resolver el contrato, en los siguientes casos:

- ✓ Por acumulación del monto máximo de la penalidad por mora o por el monto máximo para otras penalidades, en la ejecución de la prestación a su cargo.
- ✓ Caso fortuito o fuerza mayor que imposibilite la continuación del contrato.
- ✓ Incumplimiento de obligaciones contractuales, por causa atribuible al contratista.
- ✓ Hecho sobreviniente al perfeccionamiento del contrato, de supuesto distinto al caso fortuito o fuerza mayor, no imputable a ninguna de las partes, que imposibilite la continuación del contrato.
- ✓ Por incumplimiento de la cláusula anticorrupción y antisoborno.
- ✓ Por la presentación de documentación falsa o inexacta durante la ejecución contractual.

14. OBLIGACION ANTICORRUPCION Y ANTISOBORNO

A la suscripción del contrato o de la formalización de la Orden, el Contratista declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o entrega de cualquier beneficio o incentivo ilegal, de manera directa o indirecta, al (los) evaluador (es) del proceso de contratación o cualquier servidor de Hospital Regional Cusco.

Asimismo, el Contratista se obliga a mantener una conducta proba e íntegra durante la vigencia del contrato, y después de culminado el mismo en caso existan controversias pendientes de resolver, lo que supone actuar con probidad, sin cometer actos ilícitos, directa o indirectamente. Aunado a ello, el Contratista se obliga a abstenerse de ofrecer, negociar, prometer o dar regalos, cortesías, invitaciones, donativos o cualquier beneficio o incentivo ilegal, directa o indirectamente, a funcionarios públicos, servidores públicos, locadores de servicios o proveedores de servicios del área usuaria, de la dependencia encargada de la contratación, actores del proceso de contratación y/o cualquier servidor de la entidad contratante, con la finalidad de obtener alguna ventaja indebida o beneficio ilícito.

En esa línea, se obliga a adoptar las medidas técnicas, organizativas y/o de personal necesarias para asegurar que no se practiquen los actos previamente señalados.
Adicionalmente, el Contratista se compromete a denunciar oportunamente ante las autoridades competentes los actos de corrupción o de inconducta funcional de los cuales tuviera conocimiento durante la ejecución del contrato con el Hospital Regional Cusco.

Tratándose de una persona jurídica, lo anterior se extiende a sus accionistas, participacionistas, integrantes de los órganos de administración, apoderados,

representantes legales, funcionarios, asesores o cualquier persona vinculada a la persona jurídica que representa; comprometiéndose a informarles sobre los alcances de las obligaciones asumidas en virtud del presente contrato.

Finalmente, el incumplimiento de las obligaciones establecidas en este acápite, durante la ejecución contractual, otorga a Hospital Regional Cusco el derecho de resolver total o parcialmente el contrato.

15. SOLUCION DE CONTROVERSIAS

Todos los conflictos que se deriven de la ejecución e interpretación de la presente contratación, son resueltos mediante trato directo y conciliación.

16. GARANTIA COMERCIAL

La garantía del producto debe comprender el periodo de las licencias adquiridas.