SOLICITUD DE COTIZACIÓN Nº 000798

UNIDAD EJECUTORA : 002 REGION CUSCO -PLAN COPESCO
NRO. IDENTIFICACIÓN : 000790
Nº E/M : 00657

Señores : **R.U.C. :**
Dirección :
Teléfono : **Fax :**
Email : **Fecha :** 06/10/2025 **Moneda :** S/.
Concepto : SOFTWARE ANTIVIRUS CORPORATIVO - META 0010

CANTIDAD REQUERIDA	UNIDAD MEDIDA	ITEM	DESCRIPCION	PRECIO UNITARIO	PRECIO TOTAL
1	UNIDAD	140400031574	SOFTWARE (INC. LICENCIA) ANTIVIRUS CORPORATIVO		
				TOTAL	

Las cotizaciones a valores referenciales deben estar dirigidas a REGION CUSCO -PLAN COPESCO

Condiciones de Compra
- Forma de Pago:
- Garantía:
- Plazo de Entrega en Nº Dias/ Ejecución del Servicio :
- Tipo de Moneda :
- Validez de la cotización :
- Indicar Marca de Procedencia
- Tipo de Cambio :

Requerimientos Técnicos:
LUGAR DE ENTREGA
DIRECCION DE ENTREGA

FECHA DE COTIZACION

Atentamente;

ANEXO 14

DECLARACIÓN JURADA DEL PROVEEDOR

Señores:
OFICINA DE ABASTECIMIENTOS Y SERVICIOS AUXLIARES
PLAN COPESCO
Plaza Túpac Amaru s/n Huanchac
Presente.-

El que suscribe…….. identificado con DNI N° ……., y RUC N° …….. N° Tel Cel ……..
DECLARO BAJO JURAMENTO, lo siguiente:

1. *No haber incurrido, me obligo a no incurrir en actos de corrupción, así como a respetar el principio de integridad.*
2. *No tengo impedimento para contratar en el Estado.*
3. *No tengo impedimento por vínculo de parentesco hasta el segundo grado de consanguineidad, ni segundo grado de afinidad con los funcionarios de la entidad o intervinientes, según lo previsto en el artículo 11° de la Ley General de Contrataciones Públicas.*
4. *Cuento y Acepto con las condiciones necesarias para cumplir cabalmente con las características técnicas, requisitos y condiciones establecidas en los términos de referencia y/o especificaciones técnicas de la presente contratación.*
5. *De ser seleccionados para la contratación, me comprometo a mantener mi oferta en su integridad hasta el pago.*
6. *Me someto a las sanciones contenidas en la Ley General de Contrataciones Publicas, ley 32069 y su reglamento, así como la ley de procedimiento administrativo general, Ley N° 27444, cuando corresponde.*
7. *En caso de incumplimiento injustificado, acepto de manera supletoria, la aplicación de penalidad de acuerdo a la fórmula establecida en el artículo 120° del reglamento de la ley General de Contrataciones Públicas, aprobado mediante D.S N° 009-2025-EF.*
8. *De ser seleccionados para efectuar la presente contratación, autorizo al gobierno Regional del Cusco a efectos de que me pueda notificar al* ***correo electrónico*** *……o a mi domicilio sito en ……*
9. *No ser propietario, socio, representante legal, gerente general o tener cualquier vínculo con otra empresa que cotiza por el mismo objeto de término de referencia al que me presento.*

FIRMA Y SELLO DEL PROVEEDOR

CARTA AUTORIZACIÓN

PARA EL PAGO CON ABONOS EN LA CUENTA BANCARIA DEL PROVEEDOR

(Modelo: anexo N°1 de la Directiva de Tesorería)

Cusco,_____de_____del 2025.

Señores :
PLAN COPESCO

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 : .....
- CCI DE LA CUENTA BANCARIA :

- 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 y sello, según corresponda

Plaza Tupac Amaru S/N – Wánchaq – Cusco
Email: plancopesco@copesco.gob.pe
Central Telefónica (084) 581530

ESPECIFICACIONES TÉCNICAS PARA LA CONTRATACIÓN DE BIENES

ÁREA USUARIA	CENTRO DE TECNOLOGÍAS DE INFORMACIÓN
META PRESUPUESTARIA	010 GESTIÓN DE PROYECTOS
DENOMINACIÓN DE LA CONTRATACIÓN	ADQUISICION DE LICENCIA DE ANTIVIRUS CORPORATIVO PARA EL PLAN COPESCO

I. FINALIDAD PÚBLICA

Brindar protección a la información contenida en los equipos de cómputo y servidores de datos/aplicaciones del Plan COPESCO del Gobierno Regional del Cusco, de tal manera que se cuente con servicios de tecnologías de forma continua para el logro de objetivos de la Entidad

II. OBJETIVO DE LA CONTRATACIÓN

A. OBJETIVO GENERAL:

- Contar con un antivirus corporativo que permitirá la seguridad y protección de la información y aplicativos informáticos.

B. OBJETIVOS ESPECÍFICOS:

- Proteger la información de la Entidad.
- Contar con una consola de administración central para el control y monitoreo de la solución.
- Contar con antivirus cliente licenciado para cada equipo de cómputo desplegado en el parque informático de la entidad.

III. DESCRIPCIÓN Y CARACTERÍSTICAS DEL BIEN A CONTRATAR

3.1 DESCRIPCIÓN DEL BIEN A CONTRATAR

ITEM	DESCRIPCIÓN	UNIDAD	CANT.
1	Antivirus Corporativo (125 licencias) • 120 licencias de software antivirus para estaciones de trabajo más 05 licencias para servidores físicos y/o virtualizados, válido por un (01) año	UND	1

3.2 CARACTERÍSTICAS TÉCNICAS

3.2.1 CARACTERISTICAS GENERALES

- ✓ La solución deberá estar disponible totalmente en español.
- ✓ Solución de protección de próxima generación para endpoints con funcionalidades de antivirus, antimalware, anti-exploits y anti-ransomware licenciado.
- ✓ La solución debe incluir detección avanzada y respuesta acelerada automatizada (XDR).
- ✓ Deberá ser un producto reconocido en el mercado, estando presente en los tres últimos reportes de Gartner dentro del cuadrante de líderes para Plataformas de Protección Endpoint (Magic Quadrant for Endpoint Protection Platforms).
- ✓ La solución deberá permitir agregar equipos dentro de la consola utilizando al menos los siguientes métodos:
  - Sincronización con Active Directory.

PLAN COPESCO Bach. César Rubén Quispe Gómez RESPONSABLE CENTRO DE TECNOLOGÍAS DE INFORMACIÓN

PLAN COPESCO V°B° CONTROL PREVENTIVO

- Ingreso de nombre o dirección IP del equipo de manera manual.
- Tecnología propia para la detección de equipos.

✓ La solución debe proveer una serie de reportes standard de manera predeterminada.

✓ Deberán ser soluciones de propósito específico para cada tipo de dispositivo a proteger (endpoints). Es decir, un agente para endpoint y otro agente para servidores.

3.2.2 CONSOLA DE ADMINISTRACIÓN

✓ La administración deberá ser a través de una consola central única, basada en web y en sitio o en nube, que deberá contener todos los componentes para el monitoreo y control de protección de estaciones de trabajo y servidores.

✓ La consola deberá presentar un Dashboard con el resumen del estado de protección de los ordenadores y usuarios, así como indicar las alertas de eventos de criticidades alta, media e informativa.

✓ Disponer de una consola de gestión centralizada que permita la instalación, configuración, actualización y administración de todas las soluciones ofertadas de manera integral, facilitando la gestión de la seguridad.

✓ El servidor deberá contar con un módulo que detecte los equipos dentro de la red y permita tomar acciones sobre los mismos.

✓ El servidor deberá permitir la instalación remota de todas, las soluciones de

✓ seguridad de manera transparente y desatendida para el usuario.

✓ La consola debe permitir la instalación basada en componentes de acuerdo a la necesidad del usuario.

✓ La solución debe contar con mecanismo para eliminar cualquier solución de seguridad presente en las estaciones de trabajo de forma independiente o desde la consola.

✓ Debe poseer una consola de gestión centralizada que permita la instalación, configuración, actualización y administración de todas las soluciones ofertadas de manera integral, facilidad la gestión de seguridad. debe permitir administrar todos los servidores, equipos e incluso Smartphone.

✓ La consola debe permitir la asignación de roles, basada en privilegios para la delegación de responsabilidades.

✓ La solución debe permitir configurar una contraseña que impida modificación de parámetros de configuración del producto.

✓ El producto debe contar con actualizaciones compactas e incrementales que eviten la generación de archivos de gran tamaño, evitando de esta manera que pueda impactar de una manera negativa a los recursos dé ancho de banda de la red.

✓ El producto debe permitir al usuario y/o administrador de red la creación de reglas con el fin de evitar o permitir las modificaciones y accesos no autorizados en carpetas, registro del sistema, acceso a aplicaciones y archivos.

✓ La consola de administración deberá tener usuarios con distintos roles de niveles de acceso y privilegios, como administradores, operadores de la consola y usuarios de sólo lectura.

✓ Sólo los usuarios administradores podrán asignar operadores de la consola y usuarios de sólo lectura.

PLAN COPESCO
Bach. César Ruben Quispe Gómez
RESPONSABLE
CENTRO DE TECNOLOGIAS DE INFORMACIÓN

- ✓ La solución debe soportar el despliegue del producto a través de los siguientes métodos:
  - Distribución del cliente a través de GPO de Active Directory (AD) para múltiples estaciones de trabajo.
  - Instalación remota a través de la consola de administración.
  - Pre-instalado en una imagen de estación de trabajo.
  - Instalación manual a través de paquete instalador descargado desde la consola central.
  - Instalación manual a través de paquete instalador enviado vía correo electrónico a múltiples usuarios.
- ✓ Proporcionar actualizaciones del producto y de las definiciones de virus y protección contra intrusos.
- ✓ Debe permitir programar el escaneo de amenazas en las estaciones y servidores.
- ✓ Debe permitir exclusiones de escaneo para un determinado sitio Web, archivo o carpeta, aplicación o proceso. Tanto a nivel global, como específico en cada política.
- ✓ La consola de administración debe permitir la definición de grupos y sub grupos para la administración de las estaciones, usuarios y políticas.
- ✓ Posibilidad de mostrar información como nombre de la máquina, versión del antivirus, sistema operativo, dirección IP, versión del motor, fecha de la actualización, fecha de la última verificación, eventos recientes y estado.
- ✓ La herramienta de administración centralizada debe administrar todos los componentes de la protección para estaciones de trabajo y servidores y debe diseñarse para administrar, supervisar y elaborar informes de endpoint y servidores.
- ✓ La consola de administración debe incluir un panel con un resumen visual en tiempo real para comprobar el estado de seguridad.
- ✓ Deberá proporcionar filtros pre-construidos que permitan ver y corregir sólo los ordenadores que necesitan atención.
- ✓ Deberá mostrar los ordenadores administrados de acuerdo con los criterios de categoría (detalles del estado del equipo, detalles sobre la actualización, detalles de avisos y errores, detalles del antivirus, etc.), y ordenar los equipos en consecuencia.
- ✓ Permitir la ejecución manual de todos estos informes, así como la programación y envío automático por correo electrónico en los formatos CSV y PDF.
- ✓ Debe realizar envío automático de alertas críticas mediante correo electrónico a los administradores.
- ✓ El producto debe tener un módulo de control de dispositivos:
  - Permite acceso de solo lectura, lectura/escritura o bloquear dispositivos de acuerdo a una lista predefinida que incluya como mínimo: dispositivos USB, CD-ROM y dispositivos bluetooth o módems.
  - Debe tenerla capacidad de permitir que tipos de dispositivos pueden ser utilizados en el entorno de la red.
- ✓ La solución deberá incluir firewall de Windows como política.
- ✓ El firewall deberá permitir supervisar y configurar perfiles de red.

PLAN COPESCO Bach. César Ruben Quispe Gomez RESPONSABLE CENTRO DE TECNOLOGIAS DE INFORMACIÓN

PLAN COPESCO V°B° CONTROL

3.2.3 AGENTE DE PROTECCIÓN ENDPOINT

- ✓ El producto para instalación en estaciones de trabajo debe ser compatible e instalarse en su última versión sobre plataformas: Windows 8.1, Windows 10 y Windows 11.
- ✓ El producto tendrá la capacidad de desinstalar el software antivirus que se encuentre presente en el equipo de cómputo.
- ✓ El agente de instalación debe aceptar parámetros de configuración y distribución, como instalación silenciosa.
- ✓ El agente debe permitir la protección contra terminación de los procesos y servicios del producto.
- ✓ Al momento de detectar una amenaza la solución deberá permitir realizar las siguientes acciones:
  - Desinfectar
  - Enviar para análisis al fabricante
- ✓ La solución deberá contar con un sistema de prevención de intrusos basado en el host (hips).
- ✓ El agente debe permitir el uso de contraseña para prevenir la manipulación de la configuración y desinstalación del mismo por parte de cualquier usuario.
- ✓ La comunicación entre el agente y el servidor de administración debe ser mediante protocolo seguro (https).
- ✓ La solución deberá proteger todas las comunicaciones de correo electrónico que se realicen a través de alguno de los siguientes protocolos: Pop3, Imap y Mapi.
- ✓ Debe contar con un módulo que permita limitar el acceso a determinadas páginas web dependiendo de su contenido o categoría. permitir la creación de reglas para grupos de usuarios y así cumplir con las políticas de la empresa y bloquear páginas que generan un alto volumen de tráfico.

3.2.4 AGENTE DE PROTECCIÓN PARA SERVIDORES

- ✓ El producto para instalación en servidores debe ser compatible e instalarse en su última versión sobre plataformas: Microsoft Windows Server 2008R2, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 y Windows Server 2022.
- ✓ La solución deberá ser capaz de detectar todo tipo de amenazas, entre los más comunes: virus, gusanos, troyanos, spvware, adware, rootkits, bots, ransomware, etc.
- ✓ La solución deberá 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.
- ✓ La solución deberá ser capaz de crear exclusiones automáticas de los servicios que brinda al momento de la instalación, de acuerdo al tipo de servidor que este sea. y también permitir crear exclusiones manuales de escaneo ya sea por archivo, extensión o carpeta específica.
- ✓ La solución debe agregarse y ser administrado desde la consola centralizada.

3.2.5 CARACTERISTICAS BÁSICAS DE PROTECCIÓN CONTRA MALWARE

- ✓ El agente deberá proteger, detectar y prevenir amenazas en tiempo real, independientemente del estado de conexión de la estación de trabajo o servidor,

PLAN COPESCO Bach. César Ruben Quispe Gómez RESPONSABLE CENTRO DE TECNOLOGIAS DE INFORMACIÓN

PLAN COPESCO V°B° UNIDAD DE PLANEAMIENTO, PRESUPUESTO Y MODERNIZACIÓN

es decir estando online (con conexión a Internet) o en estado offline (sin conexión a Internet).

- ✓ El agente también deberá trabajar bajo demanda o programado para detectar, bloquear y limpiar todos los virus, troyanos, gusanos y spyware. En Windows, el agente también debe detectar PUA, adware y comportamiento sospechoso.
- ✓ Detección del malware en pre-ejecución y comprobar el comportamiento malicioso para detectar malware desconocido.
- ✓ Debe realizar la verificación de todos los archivos accedidos en tiempo real, incluso durante el proceso de arranque.
- ✓ Debe realizar la limpieza del sistema automáticamente, eliminando elementos maliciosos detectados y aplicaciones potencialmente indeseables (PUA).
- ✓ Debe proteger las funciones críticas en los navegadores de Internet (Safe Browsing).
- ✓ Debe permitir la autorización de detecciones maliciosas y excluir de la exploración de directorios y archivos específicos.
- ✓ Se requiere protección integrada, es decir, en un solo agente, contra amenazas de seguridad, incluyendo virus, spyware, troyanos, gusanos, adware y aplicaciones potencialmente no deseadas (PUA).
- ✓ Debe poseer la capacidad de bloqueo de ataques basado en la explotación de vulnerabilidad conocida.
- ✓ Ser capaz de aplicar un análisis adicional, inspeccionando finamente el comportamiento de los códigos durante la ejecución, para detectar el comportamiento sospechoso de las aplicaciones, tales como desbordamiento de búfer.
- ✓ Debe contar con prevención de intrusión en el host (HIPS), que monitoree el código y bloques de código que pueden comportarse de forma maliciosa antes de ser ejecutados.
- ✓ Además del control de amenazas, el mismo agente (al menos Windows) debe proporcionar control de dispositivos, control de aplicaciones, control web y prevención de fuga de información (DLP).

3.2.6 PROTECCIÓN CONTRA AMENAZAS AVANZADAS

- ✓ Protección de amenazas de día 0 a través de tecnología de deep learning (signature less).
- ✓ Funcionalidad de detección de amenazas desconocidas que están en memoria con tecnología deep learning.
- ✓ Capacidad de detección, y bloqueo proactivo de keyloggers y otros malwares no conocidos (ataques de día cero) a través del análisis de comportamiento de procesos en memoria.
- ✓ Capacidad de detección y bloqueo de troyanos (Trojans) y gusanos (Worms), entre otros malwares, por comportamiento de los procesos en memoria.
- ✓ Disponer de capacidad de protección contra ransomware no basada exclusivamente en la detección por firmas (por ejemplo: basada en comportamiento).
- ✓ No debe requerir descarga de firmas de ningún tipo.
- ✓ Bloqueo y protección contra amenazas desconocidas potencialmente sospechosas (PUA).

PLAN COPESCO Bach. César Ruben Quispe Gomez RESPONSABLE CENTRO DE TECNOLOGÍAS DE INFORMACIÓN

PLAN COPESCO V°B UNIDAD DE ASESORÍA

- ✓ Debe poseer la capacidad de bloqueo de ataques basado en la explotación de vulnerabilidades conocidas o de día cero.
- ✓ La solución debe tener capacidad de protección AMSI contra scripts maliciosos.

3.2.7 FUNCIONALIDAD DE CONTROL DE APLICACIONES

- ✓ Control de aplicaciones para monitorear e impedir que los usuarios ejecuten o instalen aplicaciones que puedan afectar la productividad o el rendimiento de la red.
- ✓ Actualización automática de la lista de aplicaciones que se pueden controlar, permitiendo aplicaciones específicas o las categorías específicas de aplicaciones que pueden ser liberadas o bloqueadas.
- ✓ Detectar aplicaciones controladas cuando los usuarios acceden, con las opciones de permitir y alertar o bloquear y alertar.

3.2.8 FUNCIONALIDAD DE CONTROL WEB

- ✓ Control de acceso a sitios web por categoría.
- ✓ El Control Web debe controlar el acceso a sitios inapropiados, con al menos 14 categorías de sitios inadecuados. También debe permitir la creación de listas blancas y listas negras.
- ✓ La aplicación de políticas de control web, debe contar con capacidad de horarios.

3.2.9 FUNCIONALIDAD DE CONTROL DE PERIFÉRICOS

- ✓ Debe permitir el monitoreo y el control de dispositivos extraíbles en los equipos de los usuarios, como dispositivos USB, periféricos de la propia estación de trabajo y redes inalámbricas, aplicando estas políticas tanto para usuarios como para dispositivo.
- ✓ El control de dispositivos debe estar al nivel de permiso, sólo lectura o bloqueo.
- ✓ Los siguientes dispositivos deben ser, como mínimo, administrados: HD (hard disks) externos, pendrives USB, almacenables removibles seguras, CD, DVD, interfaces de red inalámbrica, bluetooth, infrarrojo, MTP (Media Transfer Protocol) y PTP (Picture Transfer Protocol) como cámaras digitales.

3.2.10 FUNCIONALIDAD DE PREVENCIÓN DE FUGA DE INFORMACIÓN

- ✓ Solución de administración de archivos, asegurando que un archivo específico no salga de la Organización, buscando palabras claves o información confidencial. Se debe bloquear la carga o el envío de la información confidencial antes de enviar el archivo.
- ✓ Debe poseer protección de fugas o pérdida de datos sensibles en el mismo agente de protección, considerando su contenido, además de la posibilidad de evaluar la extensión del archivo y múltiples destinos.
- ✓ Capacidad de autorizar, bloquear y confirmar el movimiento de información sensible y en todos los casos, grabar la operación realizada con las principales informaciones de la operación.

3.2.11 SOPORTE

- ✓ En cuanto al soporte, se deberá contar tanto como con el servicio de soporte local y también de la marca presentada y deberá tenerse en cuenta lo siguiente:
- ✓ La cobertura de atención del soporte técnico deberá ser como mínimo 24x7 de la marca de lunes a domingo y del proveedor local en modalidad 8x5 (8 horas, 05 días de la semana).

PLAN COPESCO Bach. César Ruben Quispe Gómez RESPONSABLE CENTRO DE TECNOLOGÍAS DE INFORMACIÓN

PLAN COPESCO - UNIDAD FUNCIONAL DE ASESORAMIENTO V°B° CONFORME PRESENTATIVO ARQ. ITTTDR

- ✓ El periodo del soporte técnico a nivel de Software se efectuará durante el período que dure la garantía solicitada.
- ✓ El PROVEEDOR debe contar con un sistema de mesa de ayuda para el servicio de soporte técnico local para la atención de los tickets de soporte.
- ✓ Los números telefónicos y correo electrónico deben ser presentados al momento de la presentación de la propuesta técnica.
- ✓ El postor deberá indicar el procedimiento de atención, los teléfonos, horarios, correo electrónico, contactos y números preferenciales con el fabricante.
- ✓ Deberá proveerse un número telefónico de contacto (teléfono fijo), así como un correo electrónico de contacto, para la atención sobre cualquier avería, incidencia o requerimiento de la solución.

3.2.12 PRESTACIONES ACCESORIAS

- ✓ Está a cargo del proveedor la entrega de la licencia en formato digital por la cantidad de licencias solicitadas.
- ✓ El proveedor deberá realizar la instalación y configuraciones necesarias de la consola de administración, incluidas las políticas y tareas solicitadas por el Centro de Tecnologías de Información.
- ✓ El proveedor deberá realizar la instalación del antivirus en por lo menos 05 equipos clientes y 02 equipos servidores.
- ✓ El proveedor deberá realizar la capacitación en el uso y administración de la consola, la cual deberá ser certificada como mínimo para 02 trabajadores el Centro de Tecnologías de Información.
- ✓ Las capacitaciones no deberán generar costo adicional alguno a la entidad.
- ✓ La validez de la licencia deberá ser por un (01) año.

IV. MODALIDAD DE PAGO

Suma alzada

V. GARANTÍA COMERCIAL

La garantía comercial del bien será de un 01 año, contadas a partir de la fecha en que se otorga la conformidad de recepción del bien.

VI. LUGAR Y PLAZO DE EJECUCIÓN DE LA PRESTACIÓN

6.1 Lugar

El bien será entregado en el almacén central del PLAN COPESCO, ubicado en la PLAZA Tupac Amaru S/N, distrito de Wánchaq, provincia y departamento de Cusco.

6.2 Plazo

El plazo de entrega de los bienes será de 5 días calendarios computados a partir del día siguiente de la notificación de la orden de compra.

VII. FORMA Y CONDICIONES DE PAGO

7.1 Forma de pago

La forma de pago se realizará en un UNICO PAGO una vez cumplida la entrega total del bien.

7.2 Condiciones de pago

Para el pago, se realizará de acuerdo al acta de conformidad emitida por el área usuaria, el contratista deberá presentar la siguiente documentación:

- Factura
- Guía de remisión.
- Carta CCI.

PLAN COPESCO Rach. César Rubén Chirinos Gómez RESPONSABLE CENTRO DE TECNOLOGÍAS DE INFORMACIÓN

PLAN COPESCO - UPPM V°B

- Vigencia de poder, de corresponder.

VIII. CONFORMIDAD

El informe de conformidad será emitido por el responsable del Centro de Tecnologías de Información del Plan COPESCO, verificando si se ha sido cumplido con lo requerido en las especificaciones técnicas.

IX. REQUISITOS DEL PROVEEDOR

- ✓ Persona natural o jurídica.
- ✓ Contar con RUC activo y Habido
- ✓ Contar con RNP – bienes
- ✓ No encontrarse impedido de contratar con el Estado
- ✓ Proveedor dedicado al objeto de la contratación
- ✓ El proveedor debe presentar una carta original del fabricante que acredite ser distribuidor (Partner) autorizado.

X. RESPONSABILIDAD POR VICIOS OCULTOS

El plazo máximo de responsabilidad del contratista por la calidad ofrecida y por los vicios ocultos de los bienes ofertados, será de un (01) año, contados a partir de la conformidad.

XI. PENALIDADES

11.1 Penalidades

La entidad contratante puede establecer penalidades en el contrato menor. La suma de la aplicación de las penalidades por mora y de otras penalidades no puede exceder el 10% del monto del entregable correspondiente.

11.2 Penalidad por mora

Según el Art. 120 del RLGC, en caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la entidad contratante le aplica automáticamente una penalidad por mora por cada día de atraso que le sea imputable. La penalidad se aplica automáticamente y se calcula de acuerdo con la siguiente fórmula:

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

Donde F tiene los siguientes valores:
Para bienes y servicios: F= 0.40

XII. GESTIÓN DE RIESGOS

No Corresponde

XIII. OBLIGACIÓN ANTICORRUPCIÓN Y ANTISOBORNO

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 la Ley General de Contrataciones de Públicas, 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, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a estas.

Además, el proveedor se compromete a i) comunicar a las autoridades competentes, de manera

PLAN COPESCO Bach. César Ruben Quispe Gómez RESPONSABLE CENTRO DE TECNOLOGIAS DE INFORMACIÓN

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, el proveedor se compromete a no colocar a los funcionarios públicos con los que deba interactuar, en situaciones reñidas con la ética. En tal sentido, reconoce y acepta la prohibición de ofrecerles a éstos cualquier tipo de obsequio, donación, beneficio y/o gratificación, ya sea de bienes o servicios, cualquiera sea la finalidad con la que se lo haga.

XIV. SOLUCIÓN DE CONTROVERSIAS

En el caso de contratos menores, las partes pactan la conciliación como mecanismo de solución de las controversias.

XV. RESOLUCIÓN DE CONTRATO POR INCUMPLIMIENTO

Cualquiera de las partes puede resolver, total o parcialmente, el contrato en los siguientes supuestos:

a) Caso fortuito o fuerza mayor que imposibilite la continuación del contrato.
b) Incumplimiento de obligaciones contractuales, por causa atribuible a la parte que incumple.
c) Hecho sobreviniente al perfeccionamiento del contrato, de supuesto distinto al caso fortuito o fuerza mayor, no imputable a ninguna de las partes, que imposibilite la continuación del contrato.
d) Por incumplimiento de la cláusula anticorrupción.
e) Por la presentación de documentación falsa o inexacta durante la ejecución contractual.
f) Configuración de la condición de terminación anticipada establecida en el contrato, de acuerdo con los supuestos que se establezcan en el reglamento para su aplicación.

XVI. SANCIONES

El Tribunal de Contrataciones Públicas sanciona a los participantes, postores, proveedores, y subcontratistas, cuando incurran en las infracciones señaladas en el párrafo 87.1 del artículo 87 de la presente ley, sin perjuicio de las responsabilidades civiles o penales a que hubiera lugar.

Las sanciones por imponer pueden ser:

a) Multa.
b) Inhabilitación temporal.
c) Inhabilitación permanente.

La multa o inhabilitación que se impongan no eximen de la obligación de cumplir con los contratos ya perfeccionados a la fecha en que la sanción queda firme.

PLAN COPESCO Bach. Cés... Rube... Quispe Gómez RESPONSABLE CENTRO DE TECNOLOGÍAS DE INFORMACIÓN