"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la recuperación y consolidación de la economía peruana"

UE 149 - PROGRAMA DE INVERSIÓN CREACIÓN DE REDES INTEGRADAS DE SALUD

	DENOMINACIÓN	CÓDIGO
COMPONENTE	GESTIÓN	**2416127**
PRODUCTO	GESTIÓN ADMINISTRATIVA	**S/N**
ACTIVIDAD	GESTIÓN ADMINISTRATIVA	**S/N**
ACCIÓN DE INVERSION	GESTIÓN ADMINISTRATIVA	**S/N**
CONTRATO DE PRESTAMO	N° 4726/OC-PE (BID)	
NORMA DE CONTRATACIÓN APLICABLE	**Políticas para la Adquisición de Bienes y Obras Financiados por el Banco Interamericano de Desarrollo GN-2349-15**, vigentes desde enero de 2020.	

TÉRMINOS DE REFERENCIA

SUSCRIPCIÓN ANUAL DE SOFTWARE ANTIVIRUS PARA EL PROGRAMA DE INVERSIÓN CREACIÓN DE REDES INTEGRADAS DE SALUD (PCRIS)

MARZO – 2025

PCRIS Programa Creación de Redes Integradas de Salud

INDICE

1. ANTECEDENTES 3
2. ÁREA USUARIA 4
3. OBJETIVOS DE LA CONTRATACIÓN 4
4. ALCANCE Y DESCRIPCION DEL SERVICIO 4
5. ACTIVIDADES PARA REALIZAR 10
6. CONSIDERACIONES PARA LA EJECUCIÓN DEL SERVICIO 11
7. LUGAR 11
8. PLAZO DE EJECUCIÓN 11
9. RECURSOS A SER PROVISTOS POR LAS PARTES 11
10. PERFIL DEL PROVEEDOR Y SU EQUIPO DE TRABAJO 12
11. FORMA DE PAGO 12
12. COORDINACIÓN, SUPERVISIÓN Y CONFORMIDAD 13
13. PENALIDADES 13
14. RESPONSABILIDAD DEL PROVEEDOR Y SUBCONTRATACIÓN 13
15. DERECHOS DE PROPIEDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN 14
16. CONFLICTO DE INTERÉS, ELEGIBILIDAD Y PRÁCTICAS PROHIBIDAS 14

TÉRMINOS DE REFERENCIA

CONTRATACIÓN DEL SERVICIO DE SUSCRIPCIÓN ANUAL DE LICENCIAS DE SOFTWARE PARA REUNIONES VIRTUALES Y CONFERENCIA DE AUDIO Y VIDEO PARA EL PROGRAMA DE INVERSIÓN CREACIÓN DE REDES INTEGRADAS DE SALUD (PCRIS)

1. ANTECEDENTES

El 23 de octubre de 2018, el Programa Nacional de Inversiones en Salud (en adelante **PCRIS**) declaró la viabilidad del programa de inversión "Creación de Redes Integradas de Salud" (en adelante **Programa de Inversión o Programa**) con código único de inversiones N° 2416127, cuyo objetivo es lograr un adecuado acceso de la población a servicios de salud oportunos, eficientes y de calidad en el primer nivel de atención, en función a sus necesidades. Para ello, se propone rediseñar y reorganizar las Instituciones Prestadoras de Servicios de Salud (IPRESS) en Redes Integradas de Salud (RIS).

El 13 de marzo de 2019, la República del Perú suscribió con el Banco Interamericano de Desarrollo (en adelante **BID**) y el Banco Internacional de Reconstrucción y Fomento (en adelante **BIRF**), los Contratos de Préstamo N° 4726/OC-PE y N° 8920-PE, respectivamente, cada uno hasta por los citados US$ 125´000,000.00 (Ciento veinticinco millones con 00/100 dólares americanos), destinadas a financiar parcialmente al **Programa de Inversión**, más el aporte local por la suma de US$ 65'650,000.00 (Sesenta y cinco millones seiscientos cincuenta mil con 00/100 dólares americanos), haciendo un total de US$ 315´650,000.00 (Trecientos quince millones seiscientos cincuenta mil con 00/100 dólares americanos).

Mediante Decreto Supremo N° 203-2021-EF publicado el 14 de agosto de 2021, se dispuso que la Unidad Ejecutora del **Programa de Inversión** fuese el Ministerio de Salud (en adelante **MINSA**). Después, mediante Resolución Ministerial N° 1015-2021/MINSA de fecha 20 de agosto de 2021, el **MINSA** encargó al **PCRIS** la ejecución del **Programa de Inversión**, en tanto se cree una nueva Unidad Ejecutora.

Luego, mediante Oficio Nº 728-2021-EF/52.04 del 20 de agosto del 2021, la Dirección General del Tesoro Público del Ministerio de Economía y Finanzas remitió al Despacho Viceministerial de Prestaciones y Aseguramiento en Salud (en adelante **DVMPAS**) del **MINSA** una copia de las enmiendas a los citados contratos, debidamente suscritos, las mismas que establecieron que el **MINSA**, a través del Programa de Inversión "Creación de Redes Integradas de Salud" (en adelante **PCRIS),** será el Organismo Ejecutor del Programa. Las funciones del **PCRIS** en su rol de unidad ejecutora, se especificarán en el Manual Operativo del Programa.

Mediante la Resolución Ministerial N° 1177-2021/MINSA de fecha 18 de octubre de 2021 se formalizó, entre otros aspectos, la creación de la Unidad Ejecutora N° 149 - Programa de Inversión "Creación de Redes Integradas de Salud" en el pliego 011. Ministerio de Salud, la misma que se encuentra vinculada al **DVMPAS** del **MINSA.**

Mediante la Resolución de Coordinación General N° 001-2022-PCRIS-CG de fecha 4 de enero de 2022 se aprobó el Manual Operativo del **PCRIS** vigente, en concordancia con los Contratos de Préstamo N° 4726/OC-PE y N° 8920-PE, sus enmiendas y la normativa nacional aplicable.

Para el cumplimiento de objetivos del **PCRIS** se plantea mejorar la capacidad resolutiva de la oferta asistencial actual, fortalecer los sistemas de información y comunicaciones, potenciar los servicios médicos de apoyo y optimizar la cadena de suministro.

En ese marco, como una medida que permita atender los compromisos institucionales hacia el cumplimiento oportuno de los procesos relativos a la gestión administrativa del proyecto, mitigando riesgos, el Equipo de Tecnologías de la Información de la Coordinación Administrativa Financiera

requiere contar con la **CONTRATACIÓN DE SUSCRIPCIÓN ANUAL DE SOFTWARE ANTIVIRUS PARA EL PROGRAMA DE INVERSIÓN CREACIÓN DE REDES INTEGRADAS DE SALUD (PCRIS).**

2. ÁREA USUARIA

El área usuaria a cargo de la presente contratación corresponde al Equipo de Tecnologías de la Información de la Coordinación Administrativa Financiera del Programa Creación de Redes Integradas de Salud (PCRIS).

3. OBJETIVOS DE LA CONTRATACIÓN

Objetivo general

Contratar a una persona jurídica para que brinde el servicio de suscripción anual de licencias de software antivirus del PCRIS, de conformidad a los términos de referencia del presente documento.

Objetivo específico:

Fortalecer la seguridad de la información, sistemas y redes del PCRIS.

4. ALCANCE Y DESCRIPCION DEL SERVICIO

Características y condición del Servicio

DEPENDENCIA	CANTIDAD
SUSCRIPCIÓN ANUAL DE SOFTWARE ANTIVIRUS PARA EL PROGRAMA DE INVERSIÓN CREACIÓN DE REDES INTEGRADAS DE SALUD (PCRIS)	150

4.1 CARACTERÍSTICAS DE LA INFRAESTRUCTURA DE NUBE PÚBLICA

El proveedor deberá considerar el servicio de suscripción anual de licencias de antivirus que incluya las siguientes características como mínimo:

1. Ciento cincuenta (150) Licencias de Software Antivirus emitidas a nombre del PCRIS, cuya versión sea la más reciente y liberada por el fabricante, según las Características Técnicas.

2. El fabricante deberá tener soporte técnico en español y laboratorio de análisis de malware en Sudamérica para atender incidencias que afecten la región**.**

3. El software ofertado deberá ocupar una posición de Leader o Challenger en el Cuadrante Mágico de Gartner del último año de publicación.

4. El proveedor se encargará de la configuración y despliegue de la consola antivirus.

5. El proveedor se encargará del despliegue de los clientes antivirus en los usuarios finales.

6. El proveedor será responsable de la garantía, actualizaciones y soporte por un (01) año.

4.2. OTRAS CARACTERÍSTICAS

4.2.1. SOLUCIÓN DE PROTECCIÓN PARA ESTACIONES DE TRABAJO.

- 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 18.04 y superior x64, RedHat para Desktop 8, 9 x64 y superior, Linux Mint 20, 21, Apple macOS 10.12 y superior.
- 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.
- 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.
- El producto ofertado deberá permitir realizar un escaneo del equipo en modo seguro bajo línea de comando donde se podrá especificar las opciones para la limpieza de virus.
- La solución es capaz de detectar todo tipo de amenazas, entre los más comunes: virus, gusanos, troyanos, spyware, adware, rootkits, bots, ransomware, etc.
- La solución deberá contar con una funcionalidad antiransomware.
- 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.
- 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.
- Debe permitir elegir las unidades a escanear para los escaneos bajo demanda.
- El producto ofertado debe ser capaz de crear exclusiones de escaneo ya sea por archivo, extensión o carpeta específica.
- El producto ofertado debe pedir una contraseña ante intentos de cambio indebidos en la configuración del producto.
- 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.
- 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 o de tareas desde la consola de Administración.
- 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.
- El producto ofertado debe poseer un firewall bidireccional que contenga los siguientes modos de filtrado entre ellos, automático, interactivo, aprendizaje y modo basado en políticas, además que pueda tener la capacidad de bloquear conexiones entrantes y salientes.

- 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.
- El producto ofertado permitirá crear grupos que contengan varios vínculos URL para crear reglas de permiso y bloqueo a determinados sitios web.
- El bloqueo web deberá poder asignarse por un rango de tiempo, por grupo y por equipo.
- El producto ofertado debe tener un filtro antispam que permita integrarse con clientes como Microsoft Outlook. Esta funcionalidad debe permitir al usuario crear una lista negra o blanca de direcciones de correo.
- El producto ofertado deberá analizar protocolos de e-mail POP3, IMAP, MAPI.
- La protección del correo electrónico en el cliente debe permitir definir si se desea escanear sólo correo recibido, correo enviado o correo leído.
- 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.
- 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.
- El producto ofertado debe tener un módulo de protección en tiempo real para el acceso a la web.
- 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.
- 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.
- 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.
- 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).
- 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.
- El producto debe permitir realizar exploraciones completas mientras el equipo no está en uso, es decir que realice el escaneo cuando el equipo se encuentre bloqueado o suspendido. Esto con la finalidad de obtener un mejor rendimiento y limpieza del sistema.
- 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).

- La solución deberá poder realizar exploraciones en estado inactivo para poder brindar de esa forma, una protección proactiva mientras el equipo no está en uso.
- 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.
- 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.
- 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.
- La solución de antivirus debe ejecutar un escaneo o exploración en cualquiera de los siguientes estados en la computadora (Protector de pantalla o salvapantallas activo, Sesión de usuario bloqueada, Sesión de usuario finalizada)
- La solución deberá contar con un módulo de protección contra Botnets, este módulo debe ser capaz de detectar conexiones con servidores maliciosos.
- 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.
- La solución presentada incluirá una protección con el teclado, contra registradores de pulsaciones.

4.2.2 SOLUCIÓN DE PROTECCIÓN PARA DISPOSITIVOS MOVILES.

- La solución deberá ser compatible con sistemas operativos Android 6 (Marshmallow) o superior.
- La solución deberá proteger en tiempo real contra malware, escaneando todos los archivos entrantes y salientes del equipo.
- La solución deberá contar con una exploración bajo demanda para la desinfección confiable de la memoria integrada y de los medios intercambiables.
- La solución deberá contar con protección ante la desinstalación con una contraseña administrador.
- 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.
    - Bloquear el uso de la cámara integrada.
    - Que te notifique cuando se haya desactivado el GPS

- Notificar cuando el equipo este rooteado con el fin de prevenir el acceso indebido al sistema.

- La solución deberá permitir al administrador accionar los comandos remotos desde la consola mediante ejecución de tareas.
- La solución deberá bloquear en forma remota los dispositivos perdidos o robados.
- La solución deberá encontrar remotamente el teléfono y rastrear sus coordenadas de GPS.
- 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.
- La solución deberá poder activarse una alarma en el dispositivo que suene, incluso aunque el volumen esté en silencio.
- La solución deberá poder hacer un restablecimiento remoto de la configuración predeterminada de fábrica.
- 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.
- La solución deberá poder bloquear páginas web, aplicado mediante política de la consola administrativa.
- La solución deberá poder recibir un mensaje personalizado por parte del administrador.

4.2.3 SOLUCIÓN DE PROTECCIÓN PARA SERVIDORES

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

- La solución debe ser compatible con los siguientes sistemas operativos: Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022 cuales deben tener compatibilidad con la firma de código de Azure.
- El producto antivirus puede instalarse sobre plataformas de x64 bits RedHat Enterprise Linux (RHEL) 8 y 9; Ubuntu Server 20.04 y 22.04 LTS; Debian 11 y 12; SUSE Linux Enterprise Server (SLES) 15.
- Compatible con versiones del kernel del sistema operativo Linux 4.14 y posteriores
- 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)
- La solución es capaz de detectar todo tipo de amenazas, entre los más comunes: virus, gusanos, troyanos, spyware, adware, rootkits, bots, ransomware, etc.
- La solución deberá contar con una funcionalidad antiransomware.
- 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.

- 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.
- El producto debe ser capaz de crear exclusiones de escaneo ya sea por archivo, extensión o carpeta específica.
- El producto debe pedir una contraseña ante intentos de cambio indebidos en la configuración del producto.
- El producto debe contar con un agente que le permita ser administrado desde una consola centralizada.
- 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.
- La protección en tiempo real debe iniciarse con el sistema operativo, así como poder definir qué tipos de medios serán analizados por el módulo.
- La solución debe tener sistema de prevención de intrusiones basado en el host, (HIPS).
- El sistema HIPS debe tener los siguientes modos de configuración: automático, inteligente, interactivo, basado en políticas y aprendizaje.
- El producto debe permitir escanear archivos comprimidos.
- Debe permitir elegir las unidades a escanear para los escaneos bajo demanda.
- 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.
- 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.
- El producto ofertado debe poseer un firewall bidireccional que contenga los siguientes modos de filtrado entre ellos, automático, interactivo, aprendizaje y modo basado en políticas, además que pueda tener la capacidad de bloquear conexiones entrantes y salientes.

4.2.4 CONSOLA DE ADMINISTRACIÓN

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

- 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.
- 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.
- La consola de acceso al servidor deberá ser 100% web, siendo compatible con los siguientes navegadores: Mozilla Firefox, Microsoft SCCM, Google Chrome, Safari, Opera.
- 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.
- 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.
- El producto debe ser capaz de mostrar los equipos detectados en la red.
- La consola de administración centralizada debe tener la capacidad de mostrar los intentos de infección de virus en los equipos clientes.
- 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.
- 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.
- El producto debe permitir la instalación y desinstalación remota de la solución de seguridad con opción a desinstalar antivirus de terceros.
- El producto debe permitir la generación de reportes gráficos y personalización de estos.
- Los reportes deben ser fácilmente exportables en formatos CSV, PDF.
- 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.
- El producto debe ser capaz de generación de alertas ante un evento específico mediante el envío de un correo.
- 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.
- 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.
- 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.
- Deberá permitir la ejecución remota de scripts, batch files y paquetes personalizados de terceros a través de la consola.
- Deberá permitir generar grupos de clientes dinámicos y grupos estáticos.

4.2.5 OTROS

- El fabricante deberá tener soporte técnico en español y laboratorio de análisis de malware en Sudamérica para atender incidencias que afecten la región.
- Que tenga oficinas de la marca en Latinoamérica y presencia local en el país.

- El fabricante deberá estar presente en las 6 últimas publicaciones del Cuadrante Mágico de Gartner

5. ACTIVIDADES PARA REALIZAR

Las licencias y configuraciones deben de ser realizados en un plazo no mayor a diez (10) días calendarios, contabilizados a partir del día siguiente de emitida la Orden de Servicio.

El plazo de ejecución del servicio es de doce (12) meses, contados a partir del día siguiente de la firma del acta de activación del servicio.
La activación del servicio se refiere a la instalación y puesta en funcionamiento de todo el servicio, el cual se concretará a través de la firma del Acta de Inicio del Servicio.

6. CONSIDERACIONES PARA LA EJECUCIÓN DEL SERVICIO

6.1. CONSIDERACIONES GENERALES DE LA PRESTACIÓN DEL SERVICIO

El proveedor deberá brindar el SERVICIO DE SUSCRIPCIÓN ANUAL DE SOFTWARE ANTIVIRUS PARA EL PROGRAMA DE INVERSIÓN CREACIÓN DE REDES INTEGRADAS DE SALUD (PCRIS), por el plazo de trescientos sesenta y cinco (365) días, el cual será desplegado y configurado de forma remota, previa coordinación con el Equipo de Tecnologías de la Información.

6.2. DEL PROCEDIMIENTO DE LA SUPERVISIÓN DEL SERVICIO

El supervisor del servicio será Responsable del Equipo de Tecnologías de la Información o el que haga sus veces, el cual asumirá la supervisión de la prestación del servicio de suscripción anual.

7. LUGAR

El servicio será brindado en la Sede Central del PCRIS ubicado en Jr. Pedro Conde N° 261, distrito Lince, provincia y departamento de Lima.

8. PLAZO DE EJECUCIÓN

El plazo para la implementación del servicio de suscripción será hasta diez (10) días calendario contabilizados a partir del día siguiente de suscrito el contrato.

El plazo para la ejecución del servicio de suscripción anual es por un periodo trescientos sesenta y cinco (365) días, el mismo que dará inicio con fecha de suscrita el Acta de Inicio del Servicio.

9. RECURSOS A SER PROVISTOS POR LAS PARTES

9.1 RECURSOS A SER PROVISTOS POR EL PCRIS

El PCRIS brindará al PROVEEDOR para la prestación del servicio lo siguiente:

- Información, o contactos o reuniones o canales formales de obtención de la misma.
- Personas de contacto de la contraparte técnica y del área usuaria.

9.2 RECURSOS A SER PROVISTOS POR EL PROVEEDOR

El PROVEEDOR brindará para la prestación del servicio lo siguiente:

- Envío vía correo electrónico del sustento de activación de la Suscripción Anual de Licencias de Software Antivirus.

10. PERFIL DEL PROVEEDOR Y SU EQUIPO DE TRABAJO

10.1 PERFIL DEL PROVEEDOR

- Deberá ser una persona natural o jurídica con inscripción vigente en el Registro Nacional de Proveedores (RNP) en el rubro de servicios.
- No encontrarse impedido para contratar con el Estado, según lo dispuesto en el Artículo 11 de la Ley N° 30225 "Ley de Contrataciones del Estado".
- No estar inhabilitado por los organismos multilaterales (Banco Mundial y BID)

10.2 EXPERIENCIA DEL POSTOR

El postor debe acreditar un monto facturado acumulado equivalente a S/. 50,000 por la contratación de servicios similares al objeto de la convocatoria y/o en la actividad, durante un periodo de 8 años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran servicios similares a los siguientes:
- Software Antivirus y/o
- Licencias para activación de software y/o similares.

El postor debe contar con un nivel de partner Silver o Gold de la marca ofertada.

Acreditación:
La experiencia del proveedor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con Boucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago.

Cuando en los contratos, órdenes de compra o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicada por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de compra o de cancelación del comprobante de pago, según corresponda.

Importarte
En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que se hayan comprometido, según la promesa de consorcio.

11. FORMA DE PAGO

La Entidad se obliga a pagar la contraprestación a EL PROVEEDOR en SOLES, en un único pago, luego de la recepción formal y completa de la documentación y previa conformidad del servicio. Para tal fin se deberá contar con los siguientes documentos:

- Informe técnico de cumplimiento y estado del servicio por parte del Responsable del Equipo de Tecnologías de la Información.
- Conformidad del servicio.
- Acta de Inicio del Servicio
- Comprobante de pago.
- Declaración jurada del postor donde se indique el plazo de la suscripción a nombre del PCRIS.

La entidad debe pagar las contraprestaciones pactadas a favor del PROVEEDOR dentro de los quince (15) días calendario siguientes de la conformidad del servicio, siempre que se verifiquen las condiciones establecidas en el contrato y/u orden de servicio.

Los pagos se efectuarán mediante abono en cuenta bancaria, para estos efectos el PROVEEDOR deberá presentar una carta de autorización para depósito en cuenta, indicando su número de su Código de Cuenta Interbancaria (CCI) y el nombre del banco el cual deberá estar vinculado a su RUC.

La información a cargo del Contratista se debe presentar en Mesa de Partes Digital y/o Presencial en el Jirón Pedro Conde N°261, dicha documentación debe estar dirigida a la Unidad de Administración y Finanzas en el horario de 08:30 a 17:30 horas.

12. COORDINACIÓN, SUPERVISIÓN Y CONFORMIDAD

El supervisor del servicio será: el Responsable de Tecnologías de la Información o el que haga sus veces, responsable de la supervisión de la prestación del servicio.

El Coordinador Administrativo Financiero o el que haga sus veces, otorgará la conformidad al servicio en calidad de área usuaria, previo informe del Responsable de Tecnologías de la Información.

El área Usuaria tendrá un plazo, no mayor de diez (10) días calendario para dar conformidad a cada entregable. En caso de observaciones, el proveedor contará con un máximo de cinco (05) días calendario contados a partir de su notificación, para subsanar dichas observaciones. A pedido debidamente sustentado del proveedor, este plazo puede ser ampliado por el Área Usuaria.

13. PENALIDADES

13.1. PENALIDAD POR MORA

Si el PROVEEDOR incurre en retraso injustificado en la ejecución de las prestaciones objeto del contrato, el PCRIS le aplica automáticamente una penalidad por mora por cada día de atraso, de acuerdo a la siguiente fórmula:

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

Donde:

F = 0.25 para plazos mayores a sesenta (60) días o;
F = 0.40 para plazos menores o iguales a sesenta (60) días.

El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobada. Adicionalmente, se considera justificado el retraso y en consecuencia no se aplica penalidad, cuando el PROVEEDOR acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En este último caso la calificación del retraso como justificado por parte del PCRIS no da lugar al pago de gastos generales ni costos directos de ningún tipo.

14. RESPONSABILIDAD DEL PROVEEDOR Y SUBCONTRATACIÓN

El PROVEEDOR es responsable por errores, deficiencias, calidad ofrecida y/o vicios ocultos, por un plazo no menor de dos (2) años contados a partir de la conformidad otorgada por el PCRIS.

Asimismo, el PROVEEDOR es responsable de ejecutar la totalidad de las obligaciones a su cargo, de acuerdo con lo establecido en el contrato y sus documentos integrantes; por tanto, la contratación derivada del presente documento no es pasible de subcontratación.

15. DERECHOS DE PROPIEDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN

El PROVEEDOR acepta que en la medida de que el servicio prestado es por encargo, y el costo de su ejecución es asumida por el PCRIS; todo producto o materiales (impresos, estudios, informes, gráficos, programas, software de computación u otros), que se genere por el servicio, es de propiedad del PCRIS, no constituyéndose títulos de propiedad, derechos de autor y otro tipo de derechos para el PROVEEDOR; el mismo que a mérito de lo presente documento, cede en forma exclusiva y gratuita, sin generar retribución adicional a lo estipulado en el presente documento.

Asimismo, durante la vigencia del servicio y dentro de los dos (2) años siguientes a su término, el PROVEEDOR no podrá revelar ninguna información confidencial o de propiedad del PCRIS relacionada con los servicios, con el contrato que se generé o las actividades u operaciones del PCRIS. Toda la información a la que el PROVEEDOR tuviere acceso, durante o después de la ejecución del servicio, tendrán carácter confidencial, quedando expresamente prohibido su divulgación a terceros por parte del PROVEEDOR, a menos que el PCRIS otorgue mediante pronunciamiento escrito la autorización correspondiente.

16. CONFLICTO DE INTERÉS, ELEGIBILIDAD Y PRÁCTICAS PROHIBIDAS

Para efectos de la decisión de participar en el proceso de selección y/o aceptación de la contratación, los candidatos deberán tener en cuenta las causales de conflicto de interés, las condiciones de elegibilidad y las acciones que constituyen prácticas prohibidas establecidas en las Políticas para la Adquisición de Bienes y Obras Financiados por el Banco Interamericano de Desarrollo GN-2349-15, (párr. 1.16 - 1.17), las cuales podrán ser consultadas en el link:

https://idbdocs.iadb.org/wsdocs/getdocument.aspx?docnum=EZSHARE-1132444900-23307