TERMINOS DE REFERENCIA
SUSCRIPCIÓN DE LICENCIAS DE SOFTWARE ANTIVIRUS PARA ESTACIONES DE TRABAJO DE PROVIAS DESCENTRALIZADO

Órgano y/o Unidad Orgánica	Oficina de Tecnologías de la Información
Actividad del POI:	**Actividad del POI: AOI00125002339 ACCIÓN ESTRATÉGICA: AE1.01.02 INVERSIONES y MANTENIMIENTOS PARA CONTRIBUIR A UN ADECUADO NIVEL DE SERVICIO EN LAS REDES VIALES DEPARTAMENTALES Y VECINALES EN BENEFICIO DE LOS USUARIOS**
Denominación de la contratación:	**ADQUISICIÓN DE LICENCIAS DE SOFTWARE ANTIVIRUS PARA ESTACIONES DE TRABAJO DE PROVIAS DESCENTRALIZADO**

I. FINALIDAD PÚBLICA

Permitirá garantizar resultados en detección de virus informáticos, para brindar una mejor protección la cual permitirá garantizar en los equipos de cómputo y servidores de la institución una mejor seguridad de los sistemas operativos y aplicativos.

II. OBJETIVO DE LA CONTRATACIÓN

Objetivo General: Adquisición de licencias de software antivirus para estaciones de trabajo y servidores de Provias Descentralizado.

Objetivo Específico: Garantizar la disponibilidad en integridad de la Información de la información contenida en las computadoras personales, así como en los sistemas informáticos de Provias Descentralizado a fin de garantizar su disponibilidad y confiabilidad.

III. CARACTERÍSTICAS TÉCNICAS:

3.1 Alcance y Descripción de los bienes a contratar

Ítem	Cantidad	Descripción del bien
1	700	LICENCIAS DE SOFTWARE ANTIVIRUS PARA ESTACIONES DE TRABAJO Y SERVIDORES

3.2 Protección de puntos finales para estaciones de Trabajo y Servidores

3.2.1 Características técnicas mínimas para la plataforma de protección antimalware

a. La solución antimalware deberá ser presentada en modalidad de Software as a Service (SaaS), incluyendo actualizaciones de firmas y actualizaciones de producto, teniendo disponible la última versión lanzada por el fabricante.

b. La solución antimalware deberá integrar un sistema de evaluación y administración del riesgo cibernético de las estaciones y servidores protegidos, esto con el objetivo de reducir la superficie de ataque.

c. La administración del riesgo cibernético debe alinearse como mínimo a normativas ISO/IEC 27001:2022, SOC2, NIS2, CIS v8.0 en sus reportes.

d. La administración del riesgo cibernético debe brindar información de mitigación para reducir la superficie de ataque.

e. La solución ofrecida debe ser líder en el último reporte de Forrester Wave Endpoint

Security 2023 Q4.

f. La consola de administración debe permitir la configuración y administración remota de la solución antivirus instalada en las estaciones de trabajo (Windows, Linux, Mac) y servidores (Windows y Linux).

g. El acceso a la consola de administración centralizada debe ser mediante conexión segura https.

h. Con la finalidad de elevar la seguridad de acceso a la consola de administración centralizada, este debe permitir configurar autenticación mediante un segundo factor e inicios únicos de sesión mediante proveedores de identidad.

i. La consola de administración centralizada debe permitir la gestión, el monitoreo y la generación de reportes desde un solo punto.

j. Debe tener una infraestructura de administración centralizada basada en la nube, lo cual, permitirá disminuir costos al departamento de sistemas al no requerir licencias de un sistema operativo base, hardware de computador para su implantación.

k. La solución de antivirus debe poseer un único Centro de Control la cual debe reportar el estado de la solución antivirus instaladas en las dependencias.

l. El producto debe permitir al administrador visualizar como mínimo características del equipo: Sistema Operativo y versión del mismo, nombre de la PC, dirección IP, MAC, dominio al que pertenece.

m. La consola de administración centralizada debe ser capaz de implementar múltiples políticas de seguridad.

n. La consola de administración centralizada deberá permitir una estructura jerárquica para una administración personalizada de los clientes antivirus.

o. La consola de administración centralizada deberá permitir la instalación y desinstalación remota del cliente antivirus en las estaciones de trabajo y servidores.

p. El producto debe ser capaz de generar alertas ante un evento específico mediante el envío de correo electrónico.

q. Las actualizaciones deben ser descargadas centralizadamente para que los clientes actualicen desde un cliente antivirus que replique las definiciones de virus, phishing, modelos de aprendizaje automático, motores de análisis, actualizaciones del producto.

r. Cuando algún equipo se encuentre fuera de la organización este deberá reportarse a la "consola de administración centralizada" automáticamente cuanto tenga conexión a internet.

s. Debe presentar potentes opciones de asignación de políticas: configurar la herencia y forzar la aplicación a grupos y equipos.

t. Las políticas deben permitir crear reglas de herencia de módulos y/o secciones de otras políticas para facilitar su aplicación.

u. Debe permitir programar informes que puedan enviarse automáticamente por correo electrónico a cualquier número de destinatarios.

v. Debe permitir generar informes seleccionado objetivos específicos (grupos) que puedan enviarse automáticamente por correo electrónico a cualquier número de destinatarios.

w. Exportación del resumen del informe a un archivo .PDF; y el detalle en .CSV u otros formatos.

x. Debe permitir obtener reportes granulares por categoría, módulo de protección, tecnología de detección, tipo de amenaza, nombre de amenaza.

y. La restauración y eliminación de archivos en cuarentena debe realizarse desde la

"consola de administración centralizada" o desde el cliente antivirus.

z. La "consola de administración centralizada" debe permitir la visualización del estado de la restauración o eliminación de los archivos.

aa. La "consola de administración centralizada" debe permitir la creación de usuarios para una administración basada en roles.

bb. La "consola de administración centralizada" debe permitir la creación de usuarios y seleccionar objetivos (grupos) a administrar.

cc. La "consola de administración centralizada" debe permitir que cada usuario pueda configurar el cierre automático de su sesión.

dd. Registro de actividad de los usuarios en la "consola de administración centralizada": debe mostrar un registro de las acciones para una auditoria.

ee. Debe mantener registros detallados de todas las acciones de los usuarios (creación, edición, eliminación, renombrado, inicio de sesión, reinicio de equipos y otros).

ff. Debe permitir crear un solo paquete de instalación que será utilizado para estaciones de trabajo y servidores con sistema operativo Windows.

gg. La "consola de administración centralizada" debe tener la capacidad de mostrar riesgos generados por el comportamiento de los usuarios e identificarlos.

hh. La "consola de administración centralizada" debe de tener la posibilidad de realizar diagnósticos de la solución instalada en el equipo.

ii. Capacidad de agregar o quitar módulos específicos para uno o varios clientes desde la "consola de administración centralizada".

jj. Capacidad de suspender la protección completa o de módulos específicos por un tiempo determinado en clientes desde la "consola de administración centralizada".

kk. Capacidad de detener el análisis programado cuando el equipo este uso de batería.

ll. Capacidad para establecer el uso de CPU como mínimo en aceptable y bajo en servidores Linux.

3.2.2 Características de protección mínimas

a. El administrador de la solución debe tener la posibilidad de configurar el análisis automático en tiempo real para que no analice archivos que superen un determinado tamaño en MB

b. El administrador de la solución debe tener la posibilidad de configurar el análisis automático en tiempo real y bajo demanda para que no analice archivos comprimidos que superen un determinado tamaño en MB.

c. El administrador de la solución debe tener la posibilidad de configurar el análisis en tiempo real y bajo demanda con una profundidad de al menos 15 niveles para archivos comprimidos.

d. Debe incluir un sistema de análisis heurístico del comportamiento para la detección de amenazas de día Zero.

e. La solución debe incluir una defensa proactiva contra los nuevos programas maliciosos capaz de ejecutar los archivos sospechosos en un entorno virtual local para evaluar su impacto.

f. La solución debe incluir un componente antiexploit de protección contra intentos de escalación de privilegios, accesos no autorizados en la memoria y técnicas de ataque de programación orientadas al retorno.

g. El antiexploit debe incluir como mínimo la detección de 18 técnicas de ataque.

h. El componente antiexploit debe ser configurable a aplicaciones bajo demanda.

i. La solución debe ser capaz de detectar técnicas MITRE ATT&CK de ataques de

red por fuerza bruta, movimientos laterales e identificar la IP del atacante.

j. La solución debe incluir tecnologías para la detección de ransomware para evitar en gran medida el cifrado de archivos por este tipo de ataques.
k. Las capas de protección contra ransomware deben tener la capacidad de recuperar los archivos cifrados de manera automática o bajo demanda.
l. La solución debe ser capaz de detectar ataques sin archivos
m. Debe permitir el análisis bajo demanda y en tiempo real de cualquier medio de almacenamiento de información (CD, disco duro externo, unidad compartida y otros).
n. El proceso de análisis bajo demanda se puede detener si los dispositivos de almacenamiento externo contienen más de una determinada cantidad megabytes de información.
o. Análisis automático de mensajes de correo electrónico a nivel de estación de trabajo, independientemente del cliente de correo electrónico, tanto para enviados como para recibidos analizando protocolos POP3 y SMTP como mínimo.
p. Configuración de rutas que se analizaran hasta el nivel de archivo.
q. La solución debe permitir definir listas de exclusiones de análisis, tanto para tiempo real y bajo demanda como mínimo: carpetas, archivos, extensiones, hash de archivo, líneas de comando.
r. Para una mayor protección, la solución debe tener al menos tres capas de detección: basada en firmas, análisis heurístico por comportamiento y análisis continuo de procesos.
s. La solución debe permitir la exportación e importación de listas de exclusiones.
t. Para una mayor protección de las estaciones de trabajo, la solución debe analizar comunicaciones http y https.
u. Para una mejor administración de la solución instalada en las estaciones de trabajo y servidores, el producto incluirá la opción de establecer una contraseña para proteger contra la desinstalación no autorizada.
v. Para seguridad de los usuarios la solución debe contar con protección antiphishing y fraude que comprobara los enlaces contenidos en correo electrónico y buscadores.
w. La protección antiphishing debe permitir definir una lista de exclusiones URL
x. El producto debe ser capaz de evitar que sus procesos, servicios, archivos y registros pueden ser detenidos, deshabilitados, eliminados o modificados, para de esta manera garantizar su funcionamiento ante cualquier tipo de ataque de virus.
y. Debe permitir el análisis de archivos de mensajes de correos y bases de datos de correo incluyendo como mínimo los siguientes formatos: eml, msg. pst, dbx. mbx, tbb.
z. Para una mayor protección de las estaciones de trabajo, la solución debe analizar comunicaciones http, https, RDP, SSH como mínimo
aa. El cortafuegos para estaciones de trabajo debe tener la posibilidad de establecer el "modo oculto" para que el equipo no sea visible a nivel de la red local o de internet.
bb. La solución debe incluir la detección de intrusos a nivel de host IDS.
cc. La solución debe incluir un firewall personal del mismo fabricante administrado desde la "consola de administración centralizada". Este firewall debe permitir bloquear, autorizar aplicaciones y puertos de comunicación mediante la creación de reglas por dirección IP, MAC y/o puerto tanto para el origen como destino con soporte para IPv6.
dd. La solución debe permitir el envío automático de los archivos en cuarentena al

laboratorio del fabricante.

ee. El envío de archivos se efectuará automáticamente en un intervalo de tiempo predefinido (número de horas) establecido por el administrador.

ff. El producto debe incluir la opción de restaurar un archivo de la cuarentena a su ubicación original permitiendo agregar una exclusión de análisis en las configuraciones de seguridad.

gg. El producto debe incluir un componente capaz de bloquear cadenas de caracteres específicos en comunicaciones HTTP y SMTP para evitar la fuga de datos confidenciales.

hh. Debe incluir un módulo integrado para el control de usuarios con las siguientes posibilidades: bloquear el acceso a internet de clientes específicos o de grupos de clientes. Bloquear el acceso a determinadas aplicaciones. Bloquear el acceso a internet durante ciertos periodos de tiempo. Permitir el acceso a ciertas páginas web establecidas por el administrador, restringir el acceso a ciertos sitios web utilizando un conjunto de reglas predeterminadas.

ii. El producto debe incluir un módulo de control de dispositivos integrado con las siguientes posibilidades: bloquear el acceso a dispositivos de almacenamiento externo, así como dispositivos de red inalámbrica, bluetooth, unidades ópticas y otros.

jj. Debe permitir crear exclusiones de dispositivos extraíbles detectados por ID de producto e ID de dispositivo.

kk. El agente de protección debe realizar un monitoreo avanzado a nivel de Kernel del sistema operativo, permitiendo la detección de comportamientos inusuales para proteger su integridad.

3.2.3 Instalación y Administración

a. Bajo consumo de recursos del sistema e instalarse en PC'S con 512MB RAM libre y Procesador Core 2 Dúo 2Ghz

b. Antes de la instalación, el administrador puede personalizar los paquetes de instalación para que incluyan solo los módulos que se deseen tales como cortafuegos, control de contenido, control de dispositivos, antiexploit, protección contra ransomware.

c. La instalación se puede llevar a cabo de diversas maneras:
   - ✓ Instalación local utilizando el paquete antivirus directamente en la estación o servidor.
   - ✓ Instalación remota desde la "consola de administración centralizada" mediante un cliente previamente instalado para minimizar el tráfico de la WAN.
   - ✓ Instalación mediante msi.

d. La "consola de administración centralizada" deberá mostrar las estaciones de trabajo que tienen instalada la solución antivirus y las estaciones de trabajo que están desprotegidas.

e. Debe permitir crear un solo paquete de instalación que será utilizado para estaciones de trabajo y servidores con sistema operativo Windows.

f. El administrador podrá sincronizar el inventario de equipos con el Directorio Activo.

g. El administrador podrá crear grupos o subgrupos a los que podrá mover las estaciones de trabajo para una organización personalizada.

h. Se debe tener la posibilidad de seleccionar que cliente realizara el descubrimiento de los equipos en la red.

i. Para equipos con bajos recursos debe permitir la implementación de un análisis

especialmente diseñado para minimizar el consumo de recursos.

3.2.4 Requisitos del Sistema Operativo

a. Soportar máquinas con arquitectura de 32 bits y 64 bits.
b. Sistemas operativos de estaciones de trabajo: Windows 11, Windows 10, Windows 8.1, Windows 8 y versiones actuales
c. Sistemas operativos de estaciones de trabajo: Mac OS X 12 y versiones actuales.
d. Sistemas operativos de servidor: Windows Server 2022, Windows Server 2019, Windows Server 2019 Core, Windows Server 2016, Windows Server 2016 Core, Windows Server 2012 R2, Windows Server 2012 y versiones actuales.

IV. REGLAMENTOS TÉCNICOS, NORMAS METROLÓGICAS Y/O SANITARIAS, REGLAMENTOS Y DEMÁS NORMAS

No corresponde

V. GARANTÍA COMERCIAL

a. Se requiere que se brinde una garantía comercial de doce (12) meses del sistema /plataforma adquirida. La garantía debe ser otorgada por el postor y confirmada por el fabricante o el representante de la marca en el país.
b. Las características de la garantía solicitada son:
   - Las garantías y soporte iniciarán su vigencia desde el momento que se otorgue la conformidad de la puesta en marcha del sistema integral, contados a partir del día siguiente de la firma del Acta de Conformidad de la Instalación.

VI. MUESTRAS

No corresponde

VII. PRESTACIONES ACCESORIAS

Se tomarán las siguientes prestaciones accesorias.

8.1. Soporte Técnico

b. Durante el período de garantía comercial, debe contar con un Centro de Operaciones de Seguridad para el servicio de Soporte Técnico 24x7x365 con línea de comunicación gratuita para la atención de todos los tickets de cambios de configuraciones de políticas en el dispositivo de seguridad.
c. El servicio de soporte técnico comprenderá la solución de cualquier tipo de evento (incidente y/o problema) que cause una interrupción parcial o total del servicio en entidad, así como a la pérdida de la calidad o degradación del mismo. A todo ello se le denominará "falla".
d. El servicio de soporte técnico comprenderá consultas, solicitudes de reportes, y solicitudes de análisis de auditoría. A todo ello se le denominará "requerimiento".
e. El servicio de soporte técnico debe incluir el análisis, actualización, corrección y documentación de fallas en la solución implementada.
f. El servicio de soporte técnico se efectuará a través de línea telefónica, correo electrónico u otros medios disponibles. Una vez recibida tal notificación, la mesa de ayuda del postor, registrará el requerimiento y/o falla del servicio y proporcionará un número de ticket.

8.2. Capacitación

a. El postor deberá considerar una capacitación basada en currícula oficial por un

mínimo de 02 horas para un grupo de seis (06) personas. La capacitación debe comprender lo relacionado a la administración, gestión, resolución de problemas y buenas prácticas de la plataforma de protección de puntos finales ofertada.

VIII. REQUISITOS DEL PROVEEDOR

CONDICIONES GENERALES

- Persona Natural o Jurídica
- Constancia de Inscripción en el Registro Nacional de Proveedores - RNP vigente.
- Contar con RUC activo y habido.
- Tener código de cuenta interbancario (CCI).

Acreditación:

A	**CAPACIDAD TÉCNICA Y PROFESIONAL**
A.1	**CALIFICACIONES DEL PERSONAL CLAVE**
A.1.1	**FORMACIÓN ACADÉMICA**
	Requisitos: **(01) Ingeniero Especialista** • Profesional titulado en: Ingeniería Electrónica y/o Telecomunicaciones y/o Sistemas y/o Redes y/o Informática. • Deberá contar con certificación vigente del fabricante de la solución ofertada. **(01) Técnico Especialista** • Técnico titulado o Bachiller en Ingeniería de Sistemas y/o Informática y/o Técnico Titulado de Comunicaciones o Redes y/o Informática y/o Desarrollo de Software y/o Computación y/o Sistemas de Información. • Deberá contar con certificación vigente del fabricante de la solución ofertada. **Acreditación:** Se acreditará con copia simple de DIPLOMA, TITULO Y/O CERTIFICADOS
A.1.2	**EXPERIENCIA DEL PERSONAL CLAVE**
	Requisitos: **(01) Ingeniero Especialista** Mínimo 2 años de experiencia como especialista en instalación y/o implementador y/ soporte en instalación de antivirus y/o soluciones antimalware y/o seguridad de la información. **(01) Técnico Especialista** Mínimo 1 año de experiencia como asistente en instalación y/o configuración y/o implementador y/ soporte en instalación de antivirus y/o soluciones antimalware. **Acreditación:** La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii)

		constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto. Respecto a cambios en el personal clave, el reemplazo propuesto deberá tener el mismo perfil o superior que el reemplazase, este deberá ser comunicado formalmente a la entidad con un mínimo de cinco (05) días calendarios, debiendo contar con la validación respectiva para el ingreso. La Oficina de Tecnologías de la información podrá solicitar el reemplazo del personal a cardo del servicio debido a causas debidamente sustentadas y comunicadas al contratista, el cual deberá realizar el reemplazo de dicho personal en un plazo máximo de siete (07) días calendarios de recibida la notificación.
B.	**EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD**	
		Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a S/ 39,600.00 (treinta y nueve mil seiscientos y 00/100 Soles), por la contratación de bienes o servicios iguales o similares al objeto de la convocatoria, durante los ocho (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: Venta de bienes o servicios de Licencias de Software de Antivirus y/o Renovación Anual de Licencia de Antivirus y/o suscripción Anual de Licencia de Software de Antivirus y/o. **Acreditación:** La experiencia del postor 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 voucher 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 correspondientes a un máximo de veinte (20) contrataciones.

IX. LUGAR Y PLAZO DE ENTREGA

10.1. LUGAR

El bien será entregado en la Sede Institucional de Provias Descentralizado. (Jr. Camaná Nº 678 – Piso 07, Lima 01 – Perú). En horario de lunes a viernes previa coordinación con la Oficina de Tecnología de Información – OTI.

10.2. PLAZO

10.2.1. Plazo de entrega de los bienes.

Los bienes serán entregados en un plazo no mayor a **05 días** calendario, contados a partir del día siguiente de notificada la Orden de Compra.

10.2.2. Plazo de instalación, configuración y puesta en producción

La instalación, configuración y puesta en producción será en un plazo no mayor a diez (10) días calendario, contados a partir de la entrega de los bienes.

X. CONFORMIDAD

La conformidad de la adquisición del bien se regula por lo dispuesto en el artículo 144 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado mediante Decreto Supremo N° 009-2025. La conformidad es otorgada por la Oficina de Tecnologías de la Información, en el plazo máximo de siete (07) días computados desde el día siguiente de recibido el entregable.

De existir observaciones, LA ENTIDAD CONTRATANTE las comunica al CONTRATISTA, indicando claramente el sentido de estas, otorgándole un plazo para subsanar. Si pese al plazo otorgado, EL CONTRATISTA no cumpliese a cabalidad con la subsanación, LA ENTIDAD CONTRATANTE puede otorgar al CONTRATISTA periodos adicionales para las correcciones pertinentes. En este supuesto corresponde aplicar la penalidad por mora desde el vencimiento del plazo para subsanar sin considerar los días en los que pudiera incurrir la entidad contratante para efectuar las revisiones y notificar las observaciones correspondientes.

Este procedimiento no resulta aplicable cuando los servicios manifiestamente no cumplan con las características y condiciones ofrecidas, en cuyo caso LA ENTIDAD CONTRATANTE no efectúa la recepción o no otorga la conformidad, según corresponda, debiendo considerarse como no ejecutada la prestación, aplicándose la penalidad que corresponda por cada día de atraso.

XI. FORMA Y CONDICIONES DE PAGO

El pago por el presente servicio se realizará bajo la modalidad de pago a suma alzada, previa conformidad del servicio y envío de comprobante de pago.

LA ENTIDAD CONTRATANTE se obliga a pagar la contraprestación a EL CONTRATISTA, luego de la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 144 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025EF.

Para tal efecto, el responsable de otorgar la conformidad de la prestación debe hacerlo en un plazo que no excederá de los siete (7) días contabilizados desde el día siguiente de recibido el entregable, salvo que se requiera efectuar pruebas que permitan verificar el cumplimiento de la obligación, en cuyo caso la conformidad se emite en un plazo máximo de veinte (20) días, bajo responsabilidad de dicho servidor.

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

- Documento de recepción y verificación de la entrega a la Oficina de Tecnologías de la información.

- Documento en el que conste la conformidad de la prestación efectuada suscrita por el servidor responsable de la Oficina de Tecnologías de la información.

- Comprobante de pago.

Salvo los documentos que emite la entidad contratante, es decir, de recepción y verificación, así como de conformidad, el contratista debe presentar la documentación restante vía Mesa de Partes de la Entidad, sito en Jirón Camaná 678, Cercado de Lima.

LA ENTIDAD CONTRATANTE debe efectuar el pago dentro de los diez (10) días hábiles siguientes de otorgada la conformidad de los servicios, siempre que se verifiquen las condiciones establecidas en el contrato para ello, bajo responsabilidad del servidor competente.

En caso de retraso en el pago por parte de LA ENTIDAD CONTRATANTE, salvo que se deba a caso fortuito o fuerza mayor, EL CONTRATISTA tiene derecho al pago de intereses legales conforme a lo establecido en el artículo 67 de la Ley N° 32069, Ley General de Contrataciones Públicas.

El comprobante de pago y la información requerida para gestionar el pago deberá ser presentado vía Mesa de Partes de la PVD, situado en Jirón Camaná - Piso 2, distrito de Cercado de Lima y/o de manera virtual https://apps.proviasdes.gob.pe/pvdmpv/, en el horario desde las 8:30 a 17:30 horas

XII. CONFIDENCIALIDAD (De corresponder)

La confidencialidad y reserva absoluta en el manejo de información y documentación a la que se tenga acceso relacionada con la prestación, pudiendo quedar expresamente prohibido revelar dicha información a terceros. El proveedor debe dar cumplimiento a todas las políticas y estándares definidos por la Entidad, en materia de seguridad de la información.
Esta obligación comprende la información que se entrega, como también la que se genera durante la realización de las actividades y la información producida una vez que se haya concluido la entrega de los bienes. Dicha información puede consistir en mapas, dibujos, fotografías, mosaicos, planos, informes, recomendaciones, cálculos, diagnósticos, documentos, cuadros comparativos y demás datos compilados, recibidos o entregados por el proveedor.

XIII. RESPONSABILIDAD DEL PROVEEDOR

El proveedor es el responsable por la calidad ofrecida y por los vicios ocultos del bien ofertado por un plazo no menor de un (1) año, contado a partir de la conformidad otorgada por la Entidad.

XIV. PENALIDADES POR MORA

Penalidad por Mora en la ejecución de la prestación:

En caso de retraso injustificado del proveedor 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:

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

Donde F tiene los siguientes valores:
a) Para plazos menores o iguales a sesenta (60) días, para bienes:
F = 0.40.
b) Para plazos mayores a sesenta (60) días:
b.1) Para bienes: F = 0.25.

Tanto el monto como el plazo se refieren, según corresponda, al monto vigente del contrato o ítem que debió ejecutarse o, en caso que estos involucraran obligaciones de ejecución

periódica o entregas parciales, a la prestación individual que fuera materia de retraso. Se considera justificado el retraso, cuando el proveedor acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable.

El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobado. Adicionalmente, se considera justificado el retraso y en consecuencia no se aplica penalidad, cuando EL CONTRATISTA 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 de PROVIAS DESCENTRALIZADO no da lugar al pago de gastos generales ni costos directos de ningún tipo, conforme al numeral 120.4 del artículo 120 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

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

XV. OTRO TIPO DE PENALIDADES (De corresponder)

Se podrán aplicar las siguientes penalidades:

Otras penalidades			
N°	**Supuestos de aplicación de penalidad**	**Forma de cálculo**	**Procedimiento**
1	No Cumple con el tiempo de implementación	=1% de UIT por cada día trascurrido.	Según Informe de la Supervisión
	No cumple con proveer el personal ofrecido en su propuesta, salvo hecho fortuito o fuerza mayor, debidamente acreditado, y con autorización de la Entidad.	= 2% de UIT Por cada día de incumplimiento, por cada uno	Según Informe de la Supervisión

La suma de la aplicación de las penalidades por mora y de otras penalidades no debe exceder el 10% del monto vigente del contrato o, de ser el caso, del ítem correspondiente.

Estas penalidades se deducen de los pagos a cuenta, pagos parciales o del pago o liquidación final, según corresponda; o si fuera necesario, se descuenta del monto resultante de la ejecución de la garantía de fiel cumplimiento.

XVI. RESOLUCIÓN CONTRACTUAL

Cualquiera de las partes puede resolver el contrato, de conformidad con el numeral 68.1 del artículo 68 de la Ley N° 32069, Ley General de Contrataciones Públicas.

De encontrarse en alguno de los supuestos de resolución del contrato, LAS PARTES procederán de acuerdo con lo establecido en el artículo 122 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado mediante Decreto Supremo N° 009-2025-EF.

XVII.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 Ley N° 32069, 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.

XVIII. 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 que se encuentran previstas en los impedimentos de contratar, 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 o soborno, directa o indirectamente o a través de sus socios, accionistas, participacioncitas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas que se encuentran previstas en los impedimentos de contratar.

Además, el proveedor debe comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas.

El incumplimiento de las obligaciones establecidas en estas cláusulas, durante la ejecución contractual, da el derecho a la Entidad correspondiente a resolver automáticamente y de pleno derecho el contrato, bastando para tal efecto que la Entidad remita una comunicación informando que se ha producido dicha resolución, sin perjuicio de las acciones civiles, penales y administrativas a que hubiera lugar.

XIX. MEDIDAS DE SEGURIDAD EN LA PRESTACIÓN

En caso sea necesario que el proveedor realice alguna gestión en las oficinas de la Entidad, la Entidad debe indicar los protocolos sanitarios que debe cumplir de acuerdo a la normatividad vigente y disposiciones particulares propias de la Entidad.

XX. SOLUCIÓN DE CONTROVERSIAS:

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación.

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

XXI. GESTIÓN DE RIESGOS

El contratista es responsable cumplir con todas las actividades y/o características de su entregable en las condiciones y plazos requeridos, debiendo presentar el Informe y el SCTR de corresponder.

Las partes realizan la gestión de riesgos de acuerdo con lo establecido en el presente documento, a fin de tomar decisiones informadas, aprovechando el impacto de riesgos positivos y disminuyendo la probabilidad de los riesgos negativos y su impacto durante la ejecución contractual, considerando la finalidad pública de la contratación.

Riesgo Identificado	Fase de contratación	Responsable	Probabilidad	Impacto	Medida de Control / Mitigación
Incumple con el Cambio de Disco Duro Alertado	Ejecución	Proveedor	Media	Alta	Otras Penalidades
Incumplimiento en la presentación del personal clave propuesto	Ejecución	Proveedor	Baja	Alta	Otras Penalidades
El Proveedor incumple en presentar el informe correspondiente, dentro del plazo señalado	Ejecución	Proveedor	Media	Alta	Otras Penalidades

XXII. OTRA CONSIDERACIÓN

La contratación se encuentra regulada por la Ley N° 32069 "Ley General de Contrataciones Públicas".

FIRMA DIGITAL

Firmante: MANRIQUE ALEJOS Elena Lourdes FAU 20380419247 hard
Fecha: 21/10/2025 16:07
Motivo: Firma digital

Ing. ELENA MANRIQUE ALEJOS
Coordinador Administrativo de Soporte Técnico

FIRMA DIGITAL

Firmante: ARAUJO CUADROS Klaus Joseph FAU 20380419247 hard
Fecha: 21/10/2025 16:08
Motivo: Firma digital

ING. KLAUS ARAUJO CUADROS
Jefe de la Oficina de Tecnologías de la Información