Requerimiento

Términos de Referencia

1. Órgano y/o Unidad Orgánica:	Oficina de Tecnología de la Información (OFTIN)
2. Denominación de la Contratación:	Servicio de renovación de licencia de antivirus de la Agencia Espacial del Perú
3. Objetivo del POI:	Gestión Administrativa

I. FINALIDAD PÚBLICA

Garantizar la seguridad, integridad y disponibilidad de la información institucional de la Agencia Espacial del Perú – CONIDA, mediante la renovación de las licencias de software antivirus corporativo que permiten prevenir, detectar y mitigar amenazas informáticas. Esta medida contribuye a la continuidad operativa de los servicios públicos que brinda la entidad, asegurando la protección de los activos digitales frente a ciberataques y cumpliendo con las políticas de seguridad de la información establecidas por el estado peruano.

II. OBJETIVO DE LA CONTRATACIÓN

Garantizar la continuidad operativa y seguridad de la información en la Agencia Espacial del Perú – CONIDA mediante la renovación oportuna y efectiva de las licencias del antivirus corporativo alineado con las políticas institucionales de ciberseguridad y buenas prácticas en la gestión de tecnologías de la información.

III. DESCRIPCIÓN Y CANTIDAD DEL SERVICIO

3.1. Descripción del servicio a contratar:

N°	Cantidad	Descripción del servicio
1	1	Servicio de renovación de licencia de antivirus: - Cantidad de equipos informáticos: 250 - Versión de la licencia: 2024 (incluye actualizaciones)

El Inicio de la activación de la licencia se contabilizará a partir de la solicitud de la Oficina de Tecnología de la Información (OFTIN) y posterior a su activación tendrá una duración de trecientos sesenta y cinco (365) días calendarios.

Características en la protección para estaciones de trabajo y servidores:

- La solución para estaciones de trabajo debe brindar soporte a los sistemas operativos:

  - Windows 7, Windows 8, Windows 10 y Windows 11 de 64 bits.

- Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022 de 64 bits. MAC OS x 10.4.11 o superior.
- Red Hat Enterprise Linux, CentOS, Ubuntu Server, Debian GNU/Linux, SUSE Linux Enterprise Server y Oracle Linux.

- Brindar tecnología de protección capaz de eliminar amenazas de malware tales como virus, troyanos, spyware, adware, rookits, ransomware u otro tipo de software malicioso que comprometa los sistemas de información.
- Contar con un módulo de Exploit Prevention que impida que el malware explote vulnerabilidades de los sistemas operativos o aplicaciones que se ejecutan en la red.
- Monitorear las aplicaciones mediante detección de comportamiento (Behavior Detection) para proporcionar una capa adicional de vigilancia y protección contra amenazas desconocidas.
- Brindar la capacidad de inteligencia contra amenazas asistido en la nube que permita identificar objetos como reputación de archivos, dominios, IP entre otros.
- Brindar protección avanzada contra amenazas utilizando un enfoque de aprendizaje automático predictivo conocido como Machine Learning.
- Permitir escanear archivos comprimidos.
- Permitir remediación mediante el rollback de las acciones realizadas en el equipo por un software malicioso.
- Contar con una tecnología que permita mejorar el performance de los escaneos en tiempo real, manuales o programados no realizando escaneos sobre archivos anteriormente revisados o que no hayan sido modificados.
- Permitir el cambio de configuración a "modo en la nube" para los componentes de protección ofreciendo un nivel de seguridad óptima con un impacto mínimo en los recursos de los equipos y uso de ancho de banda de Internet.
- Permitir detectar vulnerabilidades en los dispositivos que ejecuten el sistema operativo Windows y aplicaciones de terceros y Microsoft.
- Permitir detectar las aplicaciones instaladas en los dispositivos que hacen uso de los servicios en la nube.

Protección de correo electrónico:

- Debe integrarse con Microsoft Outlook.
- Debe escanear a través de los puertos SMTP, POP3, IMAP, NNTP y MAPI.
- Permitir seleccionar si se deseas escanear solo los correos entrantes o los correos entrantes y salientes.
- Tener la opción de no escanear archivos comprimidos adjuntos.

- Tener una opción de filtrado de archivos adjuntos, permitiendo especificar qué tipo de archivos serán renombrado o eliminados.

Protección web:

- Analizar la data transferida mediante los protocolos HTTP, HTTPS y FTP.
- Permitir cambiar la acción que el antivirus realizará al detectar algún archivo infectado.
- Permitir realizar exclusiones de URL para que no sean analizadas por el antivirus.
- Tener la capacidad de proteger al usuario de ataques tipo phishing.
- El antivirus debe tener una base de datos de enlaces URL que tienen contenido malicioso y que deben ser bloqueados automáticamente.

Protección de red:

- Incluir un componente de Firewall y Host Intrusion Prevention.
- Permitir crear reglas para restringir el tráfico de la red a través de puertos o protocolos específicos.
- Permitir la creación de reglas que restrinjan la actividad de las aplicaciones.
- Regular el acceso de las aplicaciones a datos confidenciales usando reputación local y en la nube sin afectar su rendimiento.
- Capacidad de reconocer las redes (zonas) en la cual se encuentra un equipo en la red.
- Capacidad de detectar ataques de red y bloquear al origen, impidiendo cualquier tipo de comunicación.
- Capacidad de generar una lista de equipos confiables o direcciones IP a los cuales el componente de protección de red módulo no bloqueará.

La solución para estaciones de trabajo debe brindar las siguientes funciones de Control:

Control de aplicaciones:

- Permitir crear reglas que autoricen o bloqueen la ejecución de aplicaciones.
- Contar con diferentes criterios para especificar las aplicaciones a bloquear, como la ruta de la carpeta que contiene el archivo ejecutable, Metadatos, Hash MD5, etc.
- Tener una lista de categorías de aplicaciones provista por el fabricante que permita una selección más organizada.
- Debe permitir tener reglas activas, inactivas o en un estado de supervisión, en donde solo audite el acceso a las aplicaciones especificadas.

- Capacidad de descubrir y bloquear aplicaciones que consumen servicios de nube, redes sociales y servicios de mensajería de correo electrónico.

Control de navegación web:

- Controlar-el acceso a sitios web en los protocolos HTTP y HTTPS.
- El componente de control web debe incluir clasificación de URLs en base a categorías que permita una selección más organizada, como por ejemplo Violencia, Chat, Redes Sociales, Pornografía, o cualquier otro contenido especificado en una lista de direcciones individuales.
- Permitir especificar los usuarios o grupos a los que se les permite o bloquee el acceso a los recursos web descritos por una regla.
- Permitir bloquear o advertir mediante notificaciones el acceso al sitio web que se considere potencialmente riesgoso o que no cumpla con las normas de productividad o buen uso del servicio.
- Tener integración con el Directorio Activo para especificar reglas por usuarios o grupos

Control de dispositivos:

- Permitir bloquear por tipo de dispositivo de acuerdo con una lista predefinida que incluya como mínimo: USB, CD-ROM o medios de almacenamiento removibles.
- Permitir añadir un nuevo tipo de dispositivo en función al ID de hardware o Cass ID.
- Tener integración con el Directorio Activo para especificar reglas por usuarios o grupos
- Permitir manejar una lista de dispositivos de confianza.
- Permitir especificar el acceso al dispositivo en modo de lectura o de lectura y escritura por usuarios.

Gestión de vulnerabilidades y parches:

- Brindar funciones de gestión para Endpoint, esta función debe soportar los sistemas operativos Windows 7, Windows 8, Windows 10 y Windows 11 de 64 bits.
- Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022 de 64 bits Debe soportar como mínimo las siguientes características:
- Permitir escanear mediante la programación de una tarea a todos los equipos de la red corporativa en busca de vulnerabilidades existentes en los sistemas operativos y aplicaciones para luego permitir distribuir los parches o actualizaciones necesarias con la finalidad de mantener la estabilidad y la seguridad de los Endpoint.
- Sincronizarse con los servidores de Microsoft que brindan el servicio de Windows Update para descargar las

actualizaciones y revisiones disponibles de los sistemas operativos y aplicaciones Microsoft para luego distribuirlas en la red.
- Contar con capacidad de realizar tareas de inventario de software de los equipos de la red de modo que los administradores puedan controlar el uso de software.
- Estar en capacidad realizar tareas el inventario de hardware en los Endpoint.
- Brindar la capacidad por medio de la Consola de Administración de obtener informes personalizados de activos de hardware y licencias de software.

PROTECCION Y ADMINISTRACION PARA EQUIPOS MOVILES.:

- El producto para dispositivos móviles debe instalarse sobre equipos con sistema operativos de Smartphone y Tablets basados en Android 4.2 o superior y iOS 10.0 o superior.
- Permitir preconfigurar y desplegar aplicaciones de manera sencilla vía Google Play, App Store o su propio Self-Service Portal.
- Ofrecer protección antimalware contra las amenazas móviles más recientes, debe incluir análisis heurístico con inteligencia de amenazas asistida en nube para Android.
- Verificación de los objetos en la memoria interna del dispositivo y en las tarjetas de expansión.
- Permitir filtro de llamadas y bloquear mensaje de texto non deseado.
- Brindar funciones antirrobo como limpiar los datos personales, localizar el dispositivo, recibir el nuevo número en caso se reemplace el SIM Card.
- Bloquear el acceso a las aplicaciones y los datos corporativos en dispositivos a los que se aplicado rooting o jailbreaking.
- Permitir navegación segura en los navegadores compatibles con Android y iOS mediante el bloqueo de sitios phishing o maliciosos.
- Configurar listas blancas y listas negras de aplicativos que se podrán ejecutar en el dispositivo Android.

PROTECCION PARA CORREO ELECTRONICO:

- Brindar protección avanzada contra amenazas para los servicios de comunicación y colaboración de Microsoft Office 365.
- Permitir la detección y prevención de amenazas avanzadas como phishing, malware, spam y archivos adjuntos no deseados en los servicios ce nube de Exchange Online, OneDrive, SharePoint Online y Teams.
- Estar integrado al servicio de Microsoft Office 365 mediante el uso de API, sin la necesidad de hacer enrutamiento del correo electrónico o cambios de registros DNS hacia otra nube pública.
- Brindar soporte para el uso de SPF (marco de políticas del remitente), DKIM (identificación por claves de dominio) y DMARC (autenticación de mensajes basado en dominios) para validar los

correos electrónicos y prevenir phishing y spam por correo electrónico.
- Contar con un centro de administración vía HTTPS que permita configurar las políticas de protección antiphishing, antimalware, antispam y filtro de archivos adjuntos no deseados en el servicio de nube de Exchange Online.
- Permitir aplicar las políticas de protección a todos los usuarios de la organización Office 365 o seleccionar a usuarios específicos.

CONSOLA DE ADMINISTRACIÓN CENTRALIZADA.

- Permitir la configuración centralizada de cada una de las características y funciones provistas por los productos de protección para estaciones de trabajo, servidores físicos o virtuales y dispositivos móviles.
- El licenciamiento debe permitir desplegar la consola de administración íntegramente en Cloud, On Premise y en infraestructura de nube pública como Microsoft Azure o AWS.
- En el caso de ser On Premise debe instalarse sobre Sistemas Operativos Windows Server 2012 o superior y bases de datos SQL, Microsoft Azure SQL y MySQL, incluyendo entornos virtualizados.
- La consola de administración deberá permitir la administración centralizada de equipos basados en Windows, Linux, Mac, Android y iOS.
- El acceso a la Consola de Administración debe ser vía protocolo HTTPS.
- El producto debe ser capaz de crear tareas de desinstalación del propio antivirus y de antivirus de terceros.
- El producto debe ser capaz de mostrar los equipos detectados en la red.
- El producto debe permitir al administrador visualizar características de la PC, tales como:

  a) Sistema Operativo y versión.
  b) Nombre de la PC y dirección IP.
  c) Dominio al que pertenece.
  d) Usuarios que han iniciado sesión el equipo.
  e) Si es máquina virtual, tipo de máquina virtual.
  f) Software instalado en el equipo
  g) Características de hardware del equipo
  h) Procesos que se están ejecutando

- La consola de administración centralizada debe tener la capacidad de mostrar los archivos detectados por la protección en los equipos clientes.
- La consola de administración debe ser capaz de poder tener múltiples políticas de seguridad, pudiendo activar una política específica ante epidemias de virus.
- El producto debe tener la capacidad de crear políticas de protección y control para los dispositivos de usuarios móviles.

- Capacidad de detectar la red en la que se encuentra la PC y contactar de manera automática al servidor de políticas y actualizaciones correspondiente.
- Capacidad de controlar a través de políticas todos los componentes ofrecidos sin necesidad de usar otras consolas adicionales o productos de terceros.
- Permitir una estructura de grupos de dispositivos de manera jerárquica para una mejor administración de los clientes antivirus.
- Las políticas de administración de grupos deben heredar las políticas de grupos con mayor jerarquía.
- Permitir la creación de políticas en modo de test para recopilar información sobre las aplicaciones que se ejecutan en la red y luego usarlas ajustar la configuración en producción.
- La consola de administración debe permitir visualizar las actualizaciones Windows y de terceros que han sido instaladas y las que aún están pendientes por instalar en los dispositivos.
- Capacidad de crear un paquete de instalación consolidado (archivo ejecutable) que puede ser accedido como recurso compartido o desde algún dispositivo extermino (CD, USB, etc.), para la instalación de todos los componentes de software de protección.
- Contar con un registro o log de los eventos administrativos o detección de malware de manera detallada.
- Permitir la delegación de tareas mediante creación de usuarios basados en MS Active Directory con distintos perfiles de administración.
- Capacidad de escanear la red por Directorio Activo, Red IP o Dominios, en busca de nuevos equipos en la red.
- Permitir la generación de reportes gráficos y personalización de los mismos y deben ser exportables a formatos XML, PDF y HTML
- Los reportes deben ser personalizados y como mínimo deben ser:

  a) Reportes de las maquinas más infectadas
  b) Reportes de virus.
  c) Reportes de Actualizaciones
  d) Reportes de ataques de red
  e) Reporte del estatus de la protección.

- La consola debe ser capaz de permitir realizar un backup de sus configuraciones realizadas y de sus registros almacenados en su base de datos.
- El producto debe ser capaz de generación de alertas ante un evento mediante el envío de un correo, o la ejecución de un archivo de lotes.
- La comunicación debe ser cifrada entre servidores y clientes, usando certificados digitales provistos por el propio fabricante.
- Las actualizaciones deben ser descargadas centralizadamente para que los clientes actualicen desde el servidor de

administración sus definiciones de malware y parches del producto.

- Permitir crear categorías de aplicaciones, para autorizarlas o bloquearlas.
- Permitir visualizar todos los archivos que hayan sido desinfectados o eliminados en los equipos clientes, y tener la opción de restaurarlos si fuera necesario.
- Permitir elegir cualquier equipo cliente como un repositorio de actualizaciones y de paquetes de instalación, con el fin de optimizar el tráfico de red especificando el ancho de banda con el sitio remoto.
- Contar con un indicador de nivel de protección de dispositivos móviles que permite evaluar el nivel de riesgo del dispositivo como alto, medio o bajo.
- Permitir auditar los cambios de configuración se aplicado por los administradores.

ENDPOINT DETECTION AND RESPONSE (EDR)

- Permitir la visibilidad en tiempo real, detección y respuesta automatizada de todas las actividades ejecutadas en los Endpoint.
- Capacidad de recopilar los datos necesarios para la resolución de problemas, sin requerir un acceso físico al punto final.
- El fabricante debe tener experiencia probada en el descubrimiento de vulnerabilidades desconocidas, APTs, campañas de ciber espionaje y malware avanzado. Para ello debe haber publicado no menos de 100 documentos sobre campañas de APT y agentes de amenazas durante el último año.
- Brindar compatibilidad y soporte a los siguientes sistemas operativos:
- Windows 7, Windows 8, Windows 10 y Windows 11 de 64 bits.
- Windows Server 2012, 2012 R2, Windows Server 2016, Windows Server 2019 y Windows Server 2022 de 64 bits.
- Deberá admitir una comunicación segura entre la consola de administración y los puntos finales con el agente EDR.
- El agente EDR puede estar integrado o no a la solución de Endpoint Security, y debe ser del mismo fabricante.
- Brindar una interface para gestionar las políticas, agentes y reportes desde la misma Consola de administración del Endpoint Security.
- Capacidad de configurar por medio de una interfaz de línea de comandos.
- La solución debe admitir la generación automática de indicadores de amenazas y/o compromiso (IoC) después de que se produzca la detección, y luego tener la capacidad de aplicar una acción de respuesta.

- Capacidad de programar el escaneo en todos los puntos finales donde se ejecute el agente EDR con la información de IoC de acuerdo con una planificación del administrador.
- La solución debe admitir la importación de IoC de terceros en formato Open IoC para su uso en el escaneo de los equipos.
- La solución debe permitir tener visibilidad detallada del incidente relacionado con la amenaza detectada en un Endpoint, el incidente debe incluir como mínimo la siguiente información:
  - Gráfico de la cadena de desarrollo de amenazas (Kill Chain).
  - Información sobre el dispositivo en el que se detecta la amenaza (nombre, dirección IP, dirección MAC, lista de usuarios, sistema operativo).
  - Información general sobre la detección, incluido el modo de detección.
  - Cambios de registro asociados a la detección.
  - Historial de presencia de archivos en el dispositivo.
  - Acciones de respuesta realizadas por la aplicación.
- La información de la cadena de desarrollo de la amenaza (Kill Chain) debe proporcionar información visual sobre los objetos involucrados en el incidente, por ejemplo, sobre los procesos ejecutados en el dispositivo, conexiones de red, bibliotecas, llave de registro entre otras.
- La información de un incidente debe presentar una vista detallada de los artefactos del sistema y los datos relacionados con el incidente para el análisis de la causa raíz como por ejemplo:
  - Proceso de spawning
  - Conexiones de red
  - Cambios en el registro
  - Descarga de archivos
  - Dropped de objetos
- Contar con un mecanismo de autodefensa para evitar que se modifique archivos relacionados con su funcionamiento como las entradas de componentes del sistema.

3.2. Actividades

- Remitir al correo electrónico ccahuana@conida.gob.pe el archivo de licencia y las contraseñas de activación.
- Brindar asesoría en el servicio de renovación de licencia de antivirus informático para los servidores, estaciones de trabajo y portátiles, sin generar costos adicionales.
- Garantizar la confidencialidad de los nombres y equipos del personal que labora en la Agencia Espacial del Perú – CONIDA.
- Contar con la capacidad para atender presencialmente los problemas eventuales que se presenten y brindan la solución sin que este genere costos. En este caso particular, en horario de oficina y este deberá acercarse a la Entidad el día hábil siguiente.
- La atención de las fallas se realizará durante los 365 días calendarios a partir la activación de las licencias de antivirus.
- Realizar a solicitud de la Entidad el traslado de la licencia de un equipo a otro sin que genere costo alguno.

- Asegurar las actualizaciones del software antivirus hasta el término de plazo contratado, que incluyen nuevas versiones y base de datos.

3.3. Reglamentos según leyes, reglamentos técnicos, normas metrológicas y/o sanitarias nacionales, reglamentos y demás normal
No aplica para la presente contratación

3.4. Impacto ambiental
No aplica para la presente contratación

3.5. Plan de trabajo
No aplica para la presente contratación

3.6. Seguros
No aplica para la presente contratación

3.7. Prestaciones accesorias a la prestación principal

3.7.1. Mantenimiento preventivo y/o correctivo
No aplica para la presente contratación

3.7.2. Soporte Técnico
El proveedor deberá brindar soporte técnico para la renovación de la licencia del antivirus, incluyendo la activación, configuración y verificación de su correcto funcionamiento, asegurando la continuidad de la protección sin interrupciones durante los 365 días calendarios posteriores a la activación de las licencias de antivirus.

3.7.3. Capacitación y/o entrenamiento
No aplica para la presente contratación

3.7.4. Garantía del servicio
El proveedor deberá brindar la garantía durante los 365 días calendarios posteriores a la activación de las licencias de antivirus

3.8. Entregables

N°	Entregable	Plazo de entrega
1	Único entregable que contendrá el Paquete de Antivirus (EDR) para 250 estaciones de trabajo y el certificado de licencia del software, los mismo que serán remitido al correo ccahuana@conida.gob.pe y mesa de parte de CONIDA	A los seis (06) días calendarios de notificado la orden de servicio

Los entregables deberán ser enviados a través de la mesa de partes virtual o mesa de partes presencial. Además, los entregables deberán estar debidamente visados, firmados y foliados en todas sus páginas.

En caso de los entregables digitales, solo se aceptarán aquellos que cuenten con firma digital o firma manuscrito (documentos que hayan sido firmados y luego escaneados). No se aceptarán documentos con firmas pegadas como imagen.

3.9. Lugar y plazo de prestación del servicio

3.9.1. Lugar

El servicio se realizará en las instalaciones de las Agencia Espacial del Perú – CONIDA, Calle Luis Felipe Villarán N° 1069 - San Isidro – Lima.

3.9.2. Plazo

El plazo de la prestación del servicio debe ser de 365 días calendarios DOCE (12) meses a partir de la solicitud de activación de las licencias por parte de la Oficina de Tecnología de la Información (OFTIN).

IV. RECURSOS A SER PROVISTOS POR EL CONTRATISTA

4.1 Requisitos del proveedor

- Registro Nacional de Proveedores (RNP) Vigente – Capítulo: (Servicios).
- Registro Único de Contribuyente (RUC) activo y habido (que se dedique al objeto de la contratación)

4.2 Requisitos del personal

4.2.1 Perfil

No aplica para la presente contratación

4.2.2 Capacitación

No aplica para la presente contratación

4.2.3 Experiencia

No aplica para la presente contratación

V. OTRAS CONSIDERACIONES PARA LA EJECUCIÓN DE LA PRESTACIÓN

5.1 Recursos y facilidades a ser provistos por la entidad

Acceso al servidor de licencias para las configuraciones requeridas, previa coordinación con la Oficina de Tecnologías de la Información (OFTIN).

5.2 Adelantos

No aplica para la presente contratación

5.3 Confidencialidad

El contratista se compromete en mantener en reserva absoluta toda la información en general a la que tenga acceso y que se encuentre relacionada con la prestación, quedando prohibido revelar dicha información a terceros; el contratista se compromete a no utilizar la información a la que tenga acceso para beneficio propio alguno o

para beneficio de terceros en cualquier modalidad y en particular en materia de cooperación.

5.4 Anticorrupción y Antisoborno

El proveedor declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o entrega de cualquier beneficio o incentivo ilegal, de manera directa o indirecta, a los evaluadores del proceso de contratación o cualquier servidor de la entidad contratante. Asimismo, el proveedor se obliga a mantener una conducta proba e íntegra durante la vigencia del contrato, y después de culminado el mismo en caso existan controversias pendientes de resolver, lo que supone actuar con probidad, sin cometer actos ilícitos, directa o indirectamente. Aunado a ello, el proveedor se obliga a abstenerse de ofrecer, negociar, prometer o dar regalos, cortesías, invitaciones, donativos o cualquier beneficio o incentivo ilegal, directa o indirectamente, a funcionarios públicos, servidores públicos, locadores de servicios o proveedores de servicios del área usuaria, de la dependencia encargada de la contratación, actores del proceso de contratación y/o cualquier servidor de la entidad contratante, con la finalidad de obtener alguna ventaja indebida o beneficio ilícito. En esa línea, se obliga a adoptar las medidas técnicas, organizativas y/o de personal necesarias para asegurar que no se practiquen los actos previamente señalados. Adicionalmente, el proveedor se compromete a denunciar oportunamente ante las autoridades competentes los actos de corrupción o de inconducta funcional de los cuales tuviera conocimiento durante la ejecución del contrato con la entidad contratante. Tratándose de una persona jurídica, lo anterior se extiende a sus accionistas, participacioncitas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o cualquier persona vinculada a la persona jurídica que representa; comprometiéndose a informarles sobre los alcances de las obligaciones asumidas en virtud del presente contrato. Finalmente, el incumplimiento de las obligaciones establecidas en esta cláusula, durante la ejecución contractual, otorga a la entidad contratante el derecho de resolver total o parcialmente el contrato. Cuando lo anterior se produzca por parte de un proveedor adjudicatario de los catálogos electrónicos de acuerdo marco, el incumplimiento de la presente cláusula conllevará que sea excluido de los Catálogos Electrónicos de Acuerdo Marco. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar.

5.5 Solución de controversia

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante la conciliación o arbitraje, según el acuerdo de las partes. Cualquiera de las partes tiene derecho a iniciar el arbitraje a fin de resolver dichas controversias dentro del plazo de caducidad previsto en la Ley N° 32069, Ley General de Contrataciones Públicas, y su Reglamento. Facultativamente, 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 arbitrajes. El Laudo

arbitral emitido es inapelable, definitivo y obligatorio para las partes desde el momento de su notificación, según lo previsto en el numeral 84.9 del artículo 84 de la Ley N° 32069, Ley General de Contrataciones Públicas. En los contratos menores, todas las controversias que pudieran derivarse entre las partes respecto a la validez, nulidad, interpretación, ejecución, terminación o eficiencia contractual serán resueltas mediante un procedimiento de conciliación, conforme a lo establecido en el numeral 81.3 del artículo 81 de las Ley N° 32069.

5.6 Resolución de contrato por incumplimiento

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 y el artículo 122 de su Reglamento.

5.7 Gestión de riesgo

Las partes realizan la gestión de riesgos de acuerdo con lo establecido en el presente contrato y los documentos que lo conforman, 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.

5.8 Propiedad intelectual

No aplica para la presente contratación

5.9 Medidas de control durante la ejecución contractual

El personal de la Oficina de Tecnologías de la Información (OFTIN) supervisará el cumplimiento de los servicios.

5.10 Conformidad de la prestación

La conformidad del servicio será otorgado por el Jefe de la Oficina de Tecnologías de la Información (OFTIN.

5.11 Forma de pago

La entidad realizará el pago de la contraprestación pactada a favor del contratista en un pago único. Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la entidad debe contar con la siguiente documentación:

- Informe de conformidad brindada por la Oficina de Tecnologías de la Información (OFTIN)
- Comprobante de pago (Factura)
- Acta de conformidad brindada por la Oficina de Tecnologías de la Información (OFTIN)
- Certificado de Licencia del software

5.12 Penalidades aplicables

- **Penalidad por mora:** En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto de la contratación, la Entidad contratante le aplica automáticamente una penalidad por mora por cada día de atraso. La penalidad se aplica automáticamente y se calcula de acuerdo con la siguiente fórmula:

Calculo de la penalidad diaria

$$\text{Penalidad diaria} = \frac{0.10 \text{ x monto}}{\text{F x plazo de vigencia}}$$

Donde:
Monto: monto de la orden de servicio
Plazo de vigencia: en días, desde la recepción de la orden de servicio por parte del contratista hasta el último día del periodo de ejecución del servicio.
F= 0.40

- **Cálculo de la penalidad a aplicar:**
  Penalidad a aplicar: Penalidad diaria x días de retraso

- Consideraciones generales:
  - El monto máximo de la penalidad por mora no superará el diez por ciento (10%) del monto de la contratación o de ser el caso del ítem correspondiente.
  - Esta penalidad se deduce de los pagos a cuenta, pagos parciales o del pago o liquidación final.
  - Superado el monto máximo de la penalidad, la Entidad puede resolver la contratación.

5.13 Responsabilidad por vicios ocultos

La responsabilidad por vicios ocultos es de un (01) año, contando a partir de la recepción conforme del servicio.

5.14 Anexos

No aplica para la presente contratación

5.15 Requisitos de calificación

- **Formación académica**
  No aplica para la presente contratación

- **Capacitación**
  No aplica para la presente contratación

- **Experiencia**

  Requisitos:
  El postor debe acreditar un monto facturado acumulado equivalente a S/ 30,000.00 (treinta mil con 00/100 Soles), por el servicio de renovación de licencia de antivirus, EDR, XDR 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.

  En el caso de postores que declaren tener la condición de micro y pequeña empresa, se acredita una experiencia de S/ 10,000.00 (Diez mil con 00/100 Soles), por la venta de bienes iguales o similares al objeto de la convocatoria, durante los cinco (5) 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. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa.

Se consideran servicios similares a los siguientes: de renovación de licenciamientos (sistemas operativos, virtualizadores, kubernetes) y/o servicio de correos en la nube.

Acreditación:
La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de compra, 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.

En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones.

En el caso de suministro, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.

En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.

Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatorio correspondiente.

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.

Importante
En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que se hayan comprometido, según la promesa de consorcio, a ejecutar el objeto materia de la convocatoria, conforme a la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".

San Isidro, 24 de Junio del 2025

Firmado Digitalmente

Firmado digitalmente por: ARBAIZA ABANTO Andre Welky FAU 20131371889 soft
Motivo: Soy el autor del documento
Fecha: 24/06/2025 12:06:10-0500

Mayor FAP
ANDRE ARBAIZA ABANTO
Jefe de Tecnologías de la Información
AGENCIA ESPACIAL DEL PERÚ - CONIDA