TÉRMINOS DE REFERENCIA

Órgano y/o Dirección:	Oficina de Administración
Actividad del POI:	Gestión Administrativa
CMN N°:	2184
Denominación de la Contratación:	Servicio de Suscripción de antivirus para el Organismo de Estudios y Diseño de Proyectos de Inversión (OEDI).

I. FINALIDAD PÚBLICA

La contratación tiene como finalidad fortalecer la seguridad informática del Organismo de Estudios y Diseño de Proyectos de Inversión (OEDI) mediante la implementación de una solución de protección antivirus para estaciones de trabajo, servidores y dispositivos móviles. Esto permitirá prevenir, detectar y responder eficazmente ante amenazas cibernéticas, garantizando la continuidad operativa, la integridad de la información y el cumplimiento de estándares de seguridad tecnológica en el marco de sus funciones institucionales.

II. OBJETIVO DE LA CONTRATACIÓN

Contratar el servicio de suscripción de antivirus con la finalidad de fortalecer la seguridad digital del Organismo de Estudios y Diseño de Proyectos de Inversión (OEDI). Este servicio permitirá implementar una solución de protección avanzada que salvaguarde los activos informáticos institucionales frente a amenazas cibernéticas, minimizando riesgos operativos y de pérdida de información.

La suscripción deberá cubrir integralmente estaciones de trabajo, servidores y dispositivos móviles utilizados por la Entidad, garantizando mecanismos de detección, prevención y respuesta en tiempo real. De este modo, se asegurará la continuidad de los servicios, así como la confidencialidad, integridad y disponibilidad de la información que gestiona el OEDI en el cumplimiento de sus funciones.

III. JUSTIFICACIÓN DE LA NECESIDAD DE LA CONTRATACIÓN

En el contexto del crecimiento sostenido de las operaciones del Organismo de Estudios y Diseño de Proyectos de Inversión (OEDI), y del consecuente aumento en el volumen y sensibilidad de la información que gestiona, se ha vuelto imprescindible contar con una solución de seguridad informática que brinde una protección integral, confiable y actualizada frente a las amenazas cibernéticas que enfrentan las instituciones del sector público.

Las herramientas de protección actualmente disponibles resultan insuficientes, ya que no cubren la totalidad de los dispositivos institucionales ni ofrecen funcionalidades avanzadas de detección y respuesta ante incidentes. Esta limitación expone a la Entidad a riesgos que comprometen la confidencialidad, integridad y disponibilidad de la información, afectando potencialmente la continuidad operativa y el cumplimiento de los objetivos institucionales. En ese sentido, se requiere implementar una solución antivirus robusta, escalable y de administración centralizada que permita mitigar vulnerabilidades y asegurar la protección de la infraestructura tecnológica del OEDI.

IV. CARACTERÍSTICAS Y CONDICIONES DEL SERVICIO A CONTRATAR

4.1 Descripción del servicio a contratar

Ítem	Cantidad	Unidad de Medida	Descripción del servicio
01	**01**	Servicio	Suscripción de Antivirus para el Organismo de Estudios y Diseño de Proyectos de Inversión (OEDI).

4.2 Actividades:

Características mínimas de la suscripción:

El software deberá cumplir con las siguientes características técnicas:

- **Solución de protección para estaciones de trabajo y servidores:**
  - La solución deberá ser compatible con los principales sistemas operativos utilizados en estaciones de trabajo y servidores, en sus versiones estables o actualizadas al momento de la implementación.
  - Todos los componentes que forman parte de la solución, de seguridad para servidores, estaciones de trabajo deben ser suministrados por un solo fabricante. No se aceptarán composiciones de productos de diferentes fabricantes.
  - Deberá ser soluciones de propósito específico para cada tipo de dispositivo a proteger (endpoints, servidores). Es decir, un agente para endpoint y otro agente para servidores.
  - La cantidad de equipos con los que cuenta la Entidad es el siguiente:
    - 100 computadoras de escritorio.
    - 3 servidores
    - 24 celulares.
  - 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.
  - 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 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.
  - El producto ofertado debe contar con mínimamente módulos de control web, control de aplicaciones, prevención de perdida de datos, control de periféricos.
  - El producto ofertado debe ser capaz de crear exclusiones de escaneo ya sea por archivo, extensión o carpeta específica.
  - 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, sin depender de aplicaciones externas o de tareas desde la consola de Administración.
- 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 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, permitir 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.
- 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.
- Debe clasificar los archivos como aplicaciones maliciosas, potencialmente no deseadas (PUA) o benignas. El aprendizaje profundo también debe centrarse en los ejecutables portátiles del sistema operativo.
- Capaz de realizar nuevos análisis de amenazas de días cero sin conexión (sin Internet).
- Debe procesar datos a través de múltiples capas de análisis, cada capa haciendo que el modelo sea considerablemente más poderoso.
- Debe ser escalable: debe poder procesar una cantidad significativamente mayor de entradas, puede predecir con precisión las amenazas y al mismo tiempo mantenerse actualizado.
- La solución deberá incorporar capacidades de aprendizaje profundo mediante modelos entrenados con herramientas avanzadas de inteligencia artificial, tales como bibliotecas de

desarrollo de uso extendido en la industria como Keras, Tensorflow y Scikit-learn

- Debe poder detectar las comunicaciones entre las computadoras finales y los servidores de comando y control involucrados en una botnet u otros ataques de malware.
- Debe poder prevenir el tráfico de red malicioso con inspección de paquetes (IPS).
- Debe poder escanear el tráfico en el nivel más bajo y bloquear amenazas antes de dañar el sistema operativo o las aplicaciones.
- Al analizar se debe poder identificar que atributos de código de un objeto son similares a archivos "Known-good" y "Known bad" con esto se puede determinar si se pueden permitir o bloquear.
- Debe contar con un sistema de registro por cada ataque o intento de ataque que se haya producido en los endpoints con información detallada del malware y el origen de la infección (explorador del sistema operativo, correo electrónico, navegador, etc.).

➢ **Solución de protección para dispositivos móviles:**

- La solución de gestión y protección de móviles debe de permitir la revisión de todos los dispositivos desde una única consola
- Debe de contar con la capacidad de ver propiedades de los dispositivos (batería, IMEI, estado, entre otras)
- Debe de poder generar reportes predefinidos con información relacionada a:
  - Inventario del dispositivo
  - Dispositivos agregados a la consola los últimos 7 días
  - Dispositivos que no han sincronizado en los últimos 7 días
  - App en todas las plataformas
  - Número de apps en todas las plataformas
  - Apps en Android
  - Detalles de malware
  - Violaciones de cumplimiento
- Se pueden definir políticas de contraseñas
- Es necesario que se puedan aplicar restricciones de características como:
  - Cámara
  - Navegador
  - WiFi
  - Bluetooth
  - Compartir datos de internet
  - Uso de repositorio de aplicaciones
- Debe permitir la creación y edición de Perfiles
- Debe de poder Bloquear / Localizar / limpiar remotamente el dispositivo.
- La solución de administración y seguridad de móviles de poder detectar de "Root"
- La solución de administración y seguridad de móviles de poder detectar el uso de "Jailbreak"
- Se debe de contar con tecnología anti-phising para links en documentos y mails

- Se debe de poder integrar con autenticación "multi-factor"
- Debe de soportar las siguientes características de Seguridad:
  - Malware /PUA en Android
  - SPAM
  - WEB
  - Web Filtering
  - "Password SAFE"
- Debe de ser compatible con sistema operativo Android 9 o superior.

➢ **Consola de administración centralizada:**

- La consola debe ser con infraestructura en la nube, implementado como un servicio SAAS o debe tener la capacidad de implementarse en forma On-premise.
- La consola de administración debe permitir administrar la protección a los equipos Workstation, servidores y dispositivos móviles.
- El contratista deberá brindar un servicio de concientización vía correo electrónico mediante la misma consola y fabricante de la solución propuesta por el periodo de un mes. Esto permitirá identificar el nivel de conocimiento en temas de Ciberseguridad a 50 usuarios críticos que indique la Entidad. Este servicio deberá tener la capacidad de personalizar las plantillas de campaña de phishing.
- La consola deberá presentar un Dashboard con el resumen del estado de protección de los ordenadores y usuarios, así como indicar las alertas de eventos de criticidades alta, media e informacional.
- Debe tener la capacidad de permitir únicamente la sincronización saliente de usuarios/grupos desde los servidores locales de Active Directory al Cloud Dashboard para la gestión de políticas.
- 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 de acceso al servidor deberá ser 100% web, siendo compatible con los siguientes navegadores: Mozilla Firefox, Microsoft Edge, Google Chrome, Safari.
- 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 permitir la generación de reportes gráficos y personalización de estos.
- Los reportes deben ser fácilmente exportables en formatos CSV, PDF.
- Los recursos del informe y el monitoreo deben ser nativos de la propia consola central de administración;
- Posibilidad de mostrar información como nombre de la máquina, versión del antivirus, sistema operativo, dirección IP, versión del motor, fecha de la actualización, fecha de la última verificación, eventos recientes y estado.

- La Consola de administración debe incluir un panel con un resumen visual en tiempo real para comprobar el estado de seguridad.
- Deberá proporcionar filtros pre-construidos que permitan ver y corregir sólo los ordenadores que necesitan atención.
- Deberá mostrar los ordenadores administrados de acuerdo con los criterios de categoría (detalles del estado del equipo, detalles sobre la actualización, detalles de avisos y errores, detalles del antivirus, etc.), y ordenar los equipos en consecuencia.
- Debe tener la capacidad de evitar que los usuarios administrativos locales o los procesos maliciosos deshabiliten la protección del endpoint.
- Debe identificar un rootkit al revisar un elemento sin sobrecargar el sistema de endpoint. Los rootkits deben detectarse de forma proactiva.
- 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.

- **Otros:**
  a) La solución ofertada deberá contar con soporte técnico en idioma español provisto por el fabricante durante el tiempo del servicio con segundo nivel y como primer nivel deberá brindar soporte técnico a través del personal clave del proveedor en la modalidad 24x7.

INSTALACION:

- La solución ofertada, incluirá la configuración de la consola de administración en la nube.
- La instalación concluirá, con el despliegue de los agentes en los sistemas que se encuentren hábiles técnicamente. Aquellos equipos inaccesibles por motivos diversos como acceso al equipo, falta de permisos de administración, falta de requerimientos de instalación entre otros, no serán tomados en cuenta para la conformidad del servicio.
- La Entidad oportunamente entregará el inventario detallado de equipos a ser instalados, el cual indicará datos como: relación de equipos (nombre de equipo, dirección IP, nombre del usuario), su ubicación, permisos de administración o credenciales, permisos formales de acceso físico a los locales, acceso al computador, entre otros que faciliten las labores, la no entrega de este inventario generará la suspensión del plazo de implementación.

4.3 Plan de trabajo

No corresponde.

4.4 Sistema de entrega para bienes y servicios.

4.4.1 Diseño de la operación y mantenimiento

No corresponde.

4.4.2 Gestión de las instalaciones

No corresponde

4.5 Seguros

No corresponde.

4.6 Recursos u obligaciones a ser provistos por la Entidad.

No corresponde

4.7 Prestaciones accesorias a la prestación principal

4.7.1 Mantenimiento preventivo y/o correctivo

No corresponde.

4.7.2 Soporte técnico

No corresponde.

4.7.3 Capacitación y/o entrenamiento

No corresponde.

4.7.4 Otras prestaciones accesorias

No corresponde.

4.8 Lugar y plazo de prestación del servicio.

4.8.1 Lugar

El servicio se ejecutará en modalidad virtual, a través de la plataforma de administración centralizada provista por el fabricante del software antivirus. La gestión, monitoreo y control de las suscripciones se realizará mediante el entorno de administración en la nube.

4.8.2 Plazo de entrega y/o ejecución del servicio

El contratista contará con un plazo máximo de diez (10) días calendario, contados a partir del día siguiente de la notificación de la Orden de Servicio, para realizar la implementación completa de las suscripciones de antivirus contratadas.
Concluida la implementación, el personal encargado de la supervisión del servicio por parte del OEDI y el contratista suscribirán el Acta de Instalación y Activación de suscripción del servicio, que acreditará el cumplimiento de las obligaciones técnicas y marcará el inicio del periodo de suscripción.

La vigencia de la suscripción del servicio será de trescientos (365) días calendario, contados a partir de la fecha de suscripción del Acta de Instalación y Activación.

4.8.3 Entregable

Deberá presentar la documentación siguiente:

- Acta de Instalación y activación del servicio de antivirus donde se indique la vigencia de los 365 días calendario, detallando la fecha de inicio y fin del servicio.

- Certificado de suscripción por el periodo contratado a nombre del Organismo de Estudios y Diseño de Proyectos de Inversión (OEDI).

  Ambos documentos deberán ser presentados como máximo a los 5 días calendario de finalizada la implementación.
- Copia de la orden de servicio.
- Factura.
- Carta de autorización CCI.

El entregable deberá ser presentado a través de Mesa de Partes virtual de la Entidad, https://sgd.oedi.gob.pe/mpvdoc/inicio.do, en los plazos y fechas establecidas en los Términos de Referencia.

V. REQUISITOS Y RECURSOS PROVISTOS POR EL PROVEEDOR

Requisitos del proveedor

- Contar con RUC activo y habido en la SUNAT.
- Registro Nacional de Proveedores en los casos que la contratación supere una (1) UIT.
- Código de cuenta interbancario (CCI).
- Persona natural y/o jurídica.
- No debe tener impedimentos para contratar con el Estado.
- Correo electrónico para efectos de notificación durante la etapa de ejecución contractual.
- Contar con una Mesa de Ayuda y un Centro de Operaciones de Seguridad (SOC) propia o tercerizado para brindar el soporte 24x7x365 incluidos domingos y feriados. El SOC propio o tercerizado deberá contar como mínimo con certificación ISO27001 y ser miembro de FIRST (Forum of Incident Response and Security Teams), la cual debe ser adjuntada en la presentación de oferta.

Experiencia del proveedor

El postor debe acreditar un monto facturado acumulado equivalente a **S/ 50,000.00 (cincuenta mil con 00/100 soles)**, por la contratación de servicios 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.

Se consideran servicios similares a los siguientes:

- Servicio o provisión de licencias de software o sistemas de control y seguridad de puntos finales.
- Servicio o provisión de licencias o suscripciones de software o sistemas de software Endpoint Protección
- Servicio o provisión de equipos de seguridad perimetral
- Servicio o provisión de licencias o suscripciones de software o sistemas de software antivirus.

- Servicio o provisión de licencias de software o sistemas de Endpoint Protection and Response – EDR.

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 diez (10) contrataciones.

Equipamiento

- **Equipamiento estratégico**
  No corresponde

- **Equipamiento no estratégico**
  No corresponde

- **Infraestructura estratégica**

  No corresponde.

- **Personal clave:**

ESPECIALISTA IMPLEMENTADOR

- Un (01) profesional titulado en Ingeniería Electrónica o Ingeniería de Informática y Sistemas o Ingeniería de Sistemas o Ingeniería de Telecomunicaciones; deberá estar colegiado y habilitado al momento de la presentación de la propuesta.
- Deberá contar con certificación "ITIL Foundation Certificate" y/o "Lead Cybersecurity Professional Certificate" y/o "Internatonal Information System Security Certification Consortium ISC2"
- Deberá contar con certificación vigente del fabricante de la solución ofertada.
- Deberá contar con experiencia mínima de dos (02) años en supervisión de proyectos de seguridad informática

ESPECIALISTA SOPORTE

- Un (01) Técnico titulado y/o Bachiller en Ingeniería Electrónica, o en Telecomunicaciones, o en Redes y Comunicaciones de Datos, o Sistemas, o Informática, o de Sistemas de Información.
- Deberá contar con certificación del fabricante a nivel especialista, ingeniero o arquitecto de la solución ofertada.
- Deberá contar con experiencia mínima de dos (02) años en la implementación y soporte de soluciones de Networking y/o Ciberseguridad.

5. OTRAS CONSIDERACIONES PARA LA EJECUCIÓN DE LA PRESTACIÓN

5.1. Adelantos

No corresponde.

5.2. Modalidades de pago

De acuerdo con el objeto contractual y lo determinado en la estrategia de contratación, la modalidad de pago es a **Suma Alzada.**

5.3. Conformidad de la prestación

El responsable de la Oficina de Administración, en calidad de área usuaria, emitirá la conformidad correspondiente una vez recibido el informe de verificación del cumplimiento de la instalación de la solución antivirus, elaborado por el Coordinador de Tecnologías de la Información o quien haga sus veces. En caso corresponda, dicha conformidad deberá señalar los días de retraso injustificado u otras penalidades en las que haya incurrido el contratista, a efectos de que el OEC proceda con la determinación del importe a penalizar.

5.4. Forma de pago

La Entidad realizará el pago de la contraprestación pactada a favor del Proveedor en función a la presentación del único entregable detallado en el numeral 4.8.3 del presente documento y de acuerdo al siguiente detalle:

ENTREGABLE	MONTO A CANCELAR (%)
Único	100% del monto contratado

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

- El entregable correspondiente.
- La conformidad emitida por el área usuaria.
- Comprobante de pago autorizado por la Sunat.

El pago se realizará con abono en la cuenta "Código de Cuenta Interbancaria" (CCI) del Proveedor, como máximo, hasta los diez (10) días hábiles luego de otorgada la conformidad por parte del área usuaria y es prorrogable, previa justificación de la demora, por cinco días hábiles.

5.5. Fórmula de reajuste

No corresponde.

5.6. Penalidades

El contrato establece la penalidad por mora y otras penalidades aplicables al Proveedor ante el incumplimiento injustificado de sus obligaciones contractuales.

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.

5.6.1. Penalidad por Mora

En caso de retraso injustificado el contratista en la ejecución de las prestaciones objeto del contrato, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso. La penalidad se aplica automáticamente y se calcula de acuerdo a la siguiente fórmula:

$$\text{Penalidad diaria} = \frac{0.10 \times \text{Monto vigente}}{F \times \text{Plazo vigente en días}}$$

Donde F tiene el siguiente valor.
F = 0.40

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 involucran obligaciones de ejecución periódica o entregas parciales, a la prestación individual que fuera materia de retraso.

5.6.2. Otras penalidades aplicables

No corresponde

5.7. Gestión de Riesgos

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. Responsabilidad por vicios ocultos

La recepción conforme de la prestación por parte de la **Entidad Contratante** no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por los artículos 69 de la Ley N° 32069, Ley General de Contrataciones Públicas y el artículo144 de su Reglamento.

El plazo máximo de responsabilidad del Proveedor es de **un (1) año** contado a partir de la conformidad otorgada por la **Entidad Contratante.**

5.9. Resolución de contrato por incumplimiento en los contratos menores

La Entidad a través de la DEC podrá requerir al Proveedor mediante carta simple el cumplimiento de sus obligaciones contractuales, otorgando para ello un plazo de uno (1) a cinco (5) días calendario. Si vencido dicho plazo, el incumplimiento continúa, la Entidad puede resolver la Orden de Compra, Orden de Servicio u Contrato en forma total o parcial, comunicando la decisión al Proveedor mediante carta simple.

La resolución de contrato puede ser de forma total o parcial. La resolución parcial sólo involucra a aquella parte del contrato afectada por el incumplimiento y siempre que dicha parte sea cuantificable, separable e independiente del

resto de las obligaciones contractuales. El apercibimiento previo y la resolución que se efectúe precisan con claridad qué parte del contrato queda resuelta, de no hacerse tal precisión, se entiende que la resolución es total.

La Entidad y/o el Proveedor puede resolver el contrato, la O/C u O/S en los siguientes casos:

- Cuando se haya llegado a acumular la sumatoria del monto máximo de la penalidad por mora y otras penalidades, en la ejecución de la prestación a cargo del Proveedor.
- Hecho sobreviniente al perfeccionamiento del contrato, de supuesto distinto al caso fortuito o fuerza mayor, no imputable a ninguna de las partes, que imposibilite la continuación del contrato.
- Incumplimiento de obligaciones contractuales, por causa atribuible a la parte que incumple.
- Caso fortuito o fuerza mayor que imposibilite la continuación del contrato.
- Por incumplimiento de la cláusula anticorrupción.
- Por la presentación de documentación falsa o inexacta durante la ejecución contractual.
- Configuración de la condición de terminación anticipada establecida en el contrato, de acuerdo con los supuestos que se establezcan en el reglamento para su aplicación.
- Por mutuo acuerdo entre las partes, siempre que dicha parte sea independiente del resto de las obligaciones contractuales y previa opinión del área usuaria, a fin de que la DEC formalice la resolución total o parcial. Debe precisarse con claridad que parte de la prestación queda resuelta, de no hacerse tal precisión se entiende que la resolución es total.

El OEDI puede resolver la orden de compra, orden de servicio y/o el contrato, sin requerir previamente el cumplimiento al Proveedor, previa opinión favorable del área usuaria, cuando se deba a la acumulación de la sumatoria del monto máximo de penalidad por mora y otras penalidades, o cuando la situación de cumplimiento no pueda ser revertida. En estos casos basta comunicar al Proveedor mediante carta simple de la DEC, vía correo electrónico, la decisión de resolver.

Mientras no resulte obligatorio la utilización de la Pladicop, las resoluciones antes señaladas, se gestionarán mediante los mecanismos señalados en los párrafos precedentes.

5.10. Solución de controversias

En los contratos menores, todas las controversias que pudieran derivarse entre las partes respecto a la validez, nulidad, interpretación, ejecución, terminación o eficacia contractual serán resueltas mediante un procedimiento de conciliación, conforme a lo establecido en el numeral 81.3 del artículo 81 de la Ley Nº 32069.

5.11. Normas Anticorrupción y Antisoborno

A la suscripción de este contrato, **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[1] 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 E**ntidad 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 E**ntidad contratante** el derecho de resolver total o parcialmente el contrato[2]. 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[3]. En ningún caso, dichas medias impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar[4]

5.12. Seguridad de la información

El Proveedor se comprometa a guardar la debida reserva sobre la información que produzcan o respecto de la cual tengan acceso como resultado de la ejecución del contrato, así como a utilizar adecuadamente la información o documentación que se les proporcione y/o que tengan acceso, siendo que puede ser destinada única y exclusivamente a efectos del cumplimiento del contrato en sí, comprometiéndose además a no compartir la misma con terceros, salvo autorización expresa de la Entidad.

Acatar y dar cumplimiento a toda norma, instrucción, acuerdo, contrato o procedimiento emitido por la Entidad con respecto al acceso y manejo de la información y las prácticas para resguardarlos.

---

[1] *Artículo 9 de la Ley N°32069, Ley General de Contrataciones Públicas.*
[2] *Literal d) del Numeral 68.1 del Artículo 68 de la Ley N°32069, Ley General de Contrataciones Públicas.*
[3] *Literal d) del artículo 274 del Reglamento de la Ley N°32069, Ley General de Contrataciones Públicas.*
[4] *Numeral 122.6 del artículo 122 del Reglamento de la Ley N°32069, Ley General de Contrataciones Públicas.*

Con la previa evaluación y conformidad respectiva, el **Organismo de Estudios y Diseño de Proyectos de Inversión – OEDI**, autorizará los accesos pertinentes a recursos o herramientas propias de la institución y que son requeridos por el Proveedor para la presente contratación, así como el Proveedor será supervisado y/o monitoreado en el desarrollo de sus actividades, si así es pertinente. Una vez finalizado el contrato, los accesos serán retirados y la información proporcionada por el **OEDI** deberá ser devuelta por el Proveedor.

5.13. Confidencialidad y propiedad intelectual

La información y material producido bajo las especificaciones técnicas de este bien, tales como: escritos, medios magnéticos, digitales, y demás documentación generados por la prestación, pasará a propiedad del Organismo de Estudios y Diseño de Proyectos de Inversión. El Proveedor deberá mantener la confidencialidad y reserva absoluta en el manejo de la información y documentación a la que se tenga acceso relacionada a la prestación.

En caso de que el Proveedor incumpla el acuerdo de confidencialidad, la Entidad, a su sola discreción podrá adoptará las acciones legales que correspondan.

5.14. Acuerdos de confidencialidad

El Proveedor se compromete a guardar reserva de la información privilegiada que conociera en el ejercicio de sus funciones, tareas y demás actividades como parte de la ejecución de la prestación, no revelando en forma oral, escrita, ni por cualquier otro medio, hechos, datos, procedimientos, documentación e información de acceso restringido (confidencial), a la que tuviera acceso a partir del inicio de las prestaciones relacionadas con el referido servicio, manteniendo la confidencialidad de la misma de manera permanente.

En caso que incumpliera con cualquiera de las obligaciones estipuladas en el presente acuerdo, el OEDI está autorizado a iniciar todas las acciones judiciales o extrajudiciales necesarias para resarcir del perjuicio, y la obligación de confidencialidad perdurará mientas la información conserve las características para considerarse Confidencial.

5.15. Anexo

No corresponde.

FUNCIONARIO SOLICITANTE	
Apellidos y Nombres:	Pedro Reyna Robles
Cargo:	Jefe(e) de la Oficina de Administración.

oedi

Firmado digitalmente por REYNA ROBLES Pedro Arturo FAU 20612528587 soft
Motivo: Soy el autor del documento
Fecha: 10.07.2025 16:44:29 -05:00

Firma Electrónica