TÉRMINOS DE REFERENCIA

Órgano y/o Dirección:	Oficina de Administración
Actividad del POI:	Gestión Administrativa
Número de CMN	CMN N°02235
Denominación de la Contratación:	Servicio de alojamiento en nube pública del Sistema de Trámite Documentario y nuevas aplicaciones institucionales del Organismo de Estudios y Diseño de Proyectos de Inversión (OEDI).

I.FINALIDAD PÚBLICA

El presente requerimiento tiene como finalidad garantizar la disponibilidad, continuidad operativa, seguridad y escalabilidad de los servicios digitales institucionales que brinda el Organismo de Estudios y Diseño de Proyectos de Inversión (OEDI), a través de la contratación de un servicio de infraestructura tecnológica basada en nube pública.
Dicha contratación permitirá alojar el Sistema de Trámite Documentario institucional y, adicionalmente, facilitará la implementación progresiva de nuevas aplicaciones desarrolladas por el OEDI, orientadas a fortalecer la gestión institucional, mejorar la eficiencia de los procesos, ampliar el acceso a servicios digitales y contribuir al cumplimiento de los objetivos estratégicos establecidos en el Plan Estratégico Institucional (PEI) y el Plan Operativo Institucional (POI).

II. OBJETIVO DE LA CONTRATACIÓN

Contar con un servicio de infraestructura tecnológica en la nube pública que permita disponer de un entorno escalable, seguro y de alta disponibilidad para el alojamiento, operación y mantenimiento del Sistema de Trámite Documentario institucional, así como para el desarrollo, despliegue y operación de nuevas aplicaciones que el OEDI implemente para fortalecer sus procesos y servicios digitales.
Este entorno tecnológico permitirá garantizar la continuidad operativa de los servicios digitales institucionales, mejorar la eficiencia en la atención de expedientes y procesos documentarios, y asegurar la disponibilidad, integridad y confidencialidad de la información manejada por el OEDI, contribuyendo al logro de los objetivos estratégicos y metas institucionales establecidas en el Plan Estratégico Institucional (PEI) y en el Plan Operativo Institucional (POI).

III. JUSTIFICACIÓN DE LA NECESIDAD DE LA CONTRATACIÓN

El Organismo de Estudios y Diseño de Proyectos de Inversión (OEDI) requiere asegurar la continuidad operativa, disponibilidad y seguridad del Sistema de Trámite Documentario institucional, herramienta fundamental para la atención de expedientes, la gestión documental y el cumplimiento de sus funciones asignadas.

Asimismo, el OEDI tiene proyectado desarrollar e implementar nuevas aplicaciones digitales que permitan modernizar y optimizar sus procesos internos y servicios orientados a los usuarios, lo que demanda contar con un entorno tecnológico flexible, escalable y alineado a las mejores prácticas de seguridad de la información.

Actualmente, la infraestructura local disponible no permite garantizar un funcionamiento estable, seguro y con la capacidad de adaptación necesaria ante incrementos en la carga de trabajo, crecimiento del número de usuarios y mayores volúmenes de información.

Por ello, resulta necesario contratar un servicio de infraestructura en nube pública que proporcione los recursos técnicos adecuados para:

- Asegurar la operación continua del Sistema de Trámite Documentario.
- Facilitar el despliegue y funcionamiento de nuevas aplicaciones institucionales.
- Garantizar la integridad, confidencialidad y disponibilidad de la información institucional.
- Contribuir al cumplimiento de los objetivos estratégicos establecidos en el Plan Estratégico Institucional (PEI) y las metas del Plan Operativo Institucional (POI).

Esta contratación permitirá fortalecer la transformación digital del OEDI, optimizar recursos y reducir riesgos asociados a la gestión de infraestructura propia.

IV. CARACTERÍSTICAS Y CONDICIONES DEL SERVICIO A CONTRATAR

Descripción del servicio a contratar:

Ítem	Descripción del servicio	Cantidad
1	Servicio de alojamiento en nube pública del Sistema de Trámite Documentario y nuevas aplicaciones institucionales del Organismo de Estudios y Diseño de Proyectos de Inversión (OEDI).	01

4.1 Actividades:

Consideraciones generales que debe tener la nube:

La infraestructura de nube ofertada, debe soportar las siguientes características:

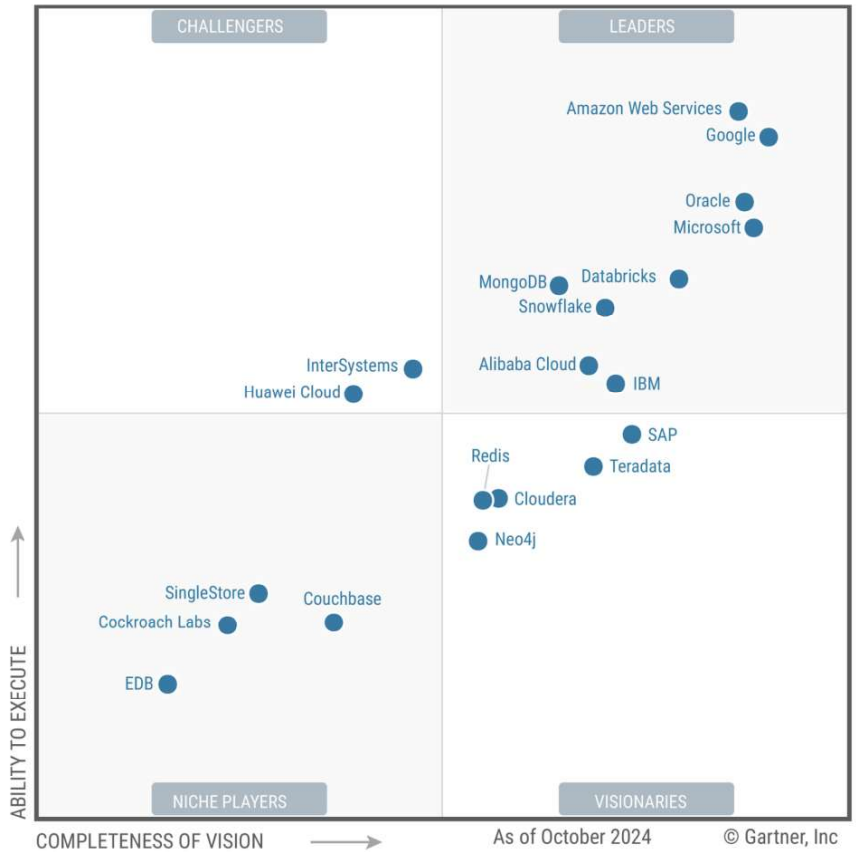
PRESTACIÓN PRINCIPAL:

4.1.1 Características técnicas de la nube publica:

El servicio de nube pública ofertado deberá contar con las siguientes características:

- El servicio debe ser brindado por un proveedor de servicios de nube pública y debe figurar dentro del Cuadrante Mágico de Gartner de Servicios de Infraestructura y Plataforma en Nube más reciente (octubre 2024).

Figure 1: Magic Quadrant for Cloud Database Management Systems



Nota: *El cuadrante de Gartner se basa en una serie de informes de investigación de mercados publicados por la consultoría de Gartner, basándose en método de análisis de datos cualitativos para demostrar madurez y visión panorámica de las posiciones relativas de sus competidores.*

- El servicio de nube pública debe contar con un catálogo oficial de servicios, disponible en la página web del proveedor, que permita el acceso público y gratuito a la descripción detallada de las características técnicas de cada servicio ofertado, sin necesidad de registro previo.
- El servicio deberá contar con una plataforma o consola la cual permita administrar los servicios de Infraestructura pública o Nube pública, la misma que será manejada por el Especialista Implementador del Servicio a contratar.
- Asegurar un tiempo de actividad (uptime) mínimo del 99.9% para la Infraestructura de Nube descrita en los presentes términos de referencial, durante el periodo de vigencia del contrato, garantizando la continuidad operativa de los servicios digitales institucionales.
- El servicio de nube debe contar con certificaciones como:
  SOC 1: Informe de controles de auditoría.
  SOC 2: Informe de seguridad, disponibilidad y confidencialidad.
  SOC 3: Informe de controles generales.
  ISO 9001: Estándar de calidad internacional.
  ISO 27001: Controles de administración de seguridad.

ISO 27017: Controles específicos de la nube.
ISO 27018: Protección de datos personales.
Los cuales deberán ser presentados junto con la oferta (cotización).

4.1.2 Servicios de gestión de identidad y acceso:

- El servicio debe permitir controlar el acceso, permisos a sus recursos y servicios de la nube.
- El servicio debe permitir que se administren permisos para sus usuarios y aplicaciones.
- El servicio debe permitir analizar el acceso a recursos y servicios.
- El servicio debe garantizar que los usuarios no tendrán acceso a los recursos de la nube hasta que se concedan de forma explícita los permisos.
- El servicio debe permitir crear credenciales temporales.
- El servicio debe permitir identificar y eliminar fácilmente los permisos no utilizados.
- El servicio debe permitir diferentes modos de autenticación de usuarios como contraseñas, pares de claves y autenticación multifactor.
- El servicio debe soportar la federación desde sistemas corporativos como Microsoft Active Directory, así como proveedores de identidad basados en estándares.
- El servicio debe permitir bloquear los puertos que dan acceso a la nube pública y generar listas blancas de direcciones IP a través políticas.
- El servicio debe permitir contar con información de auditoría de accesos a los recursos de la nube.

4.1.3 Servicios de cómputo de instancias virtuales:

- El servicio debe contar con un entorno virtual de cómputo que permita utilizar interfaces de servicios web para lanzar instancias con distintos sistemas operativos, cargarlas con su entorno de aplicaciones personalizado, administrar los permisos de acceso a la red y ejecutar su imagen utilizando los sistemas que se desee.
- El servicio debe permitir pausar y reanudar las instancias.
- El servicio debe contar con la capacidad para lanzar / administrar un grupo de recursos de cómputo con una sola solicitud.
- El servicio debe permitir hacer seguimiento de licencias para regular el uso y el cumplimiento.
- El servicio debe permitir implementar funcionalidades de auto escalamiento.
- El servicio debe contar con la capacidad de sincronización de tiempo para instancias cómputo.
- El servicio debe soportar acceso SSH basado en políticas.
- El servicio debe ser suministrado bajo un esquema de pago por uso.
- El servicio debe ofrecer la posibilidad de colocar instancias en distintas regiones de disponibilidad.
- El servicio debe permitir el uso de direcciones IP públicas.
- El servicio debe permitir ajustar la escala de la capacidad de las instancias automáticamente de acuerdo con las condiciones que se definan.
- El servicio debe permitir acceder de manera privada a la API de las instancias desde su red privada de nube o sobre conexión directa, sin utilizar IP públicas y sin que el tráfico deba atravesar la Internet.
- Debe ofrecer un servicio de origen de hora de alta precisión, fiabilidad y disponibilidad que pueda ser usado por los servicios de cómputo.

4.1.4 Servicios de base de datos relacional:

- El servicio debe permitir automatizar las tareas administrativas, como el aprovisionamiento de hardware, la configuración de bases de datos, la implementación de parches y la creación de copias de seguridad.
- El servicio debe permitir escoger entre los siguientes motores de bases de datos SQL: Mysql v8
- El servicio debe ser compatible con herramientas para migrar o replicar las bases de datos existentes.
- El servicio debe estar en capacidad de encargarse de tareas habituales de las bases de datos, como el aprovisionamiento, las revisiones, las copias de seguridad, la recuperación, la detección de errores y la reparación.
- El servicio se debe poder desplegar en múltiples centros de datos del proveedor de nube para garantizar alta disponibilidad.
- El servicio debe permitir aplicar de forma automática parches de software.
- El servicio debe contar con diversas opciones de almacenamiento en virtud del rendimiento requerido. Las opciones de almacenamiento deben incluir: Almacenamiento de uso general (SSD) y/o Almacenamiento de IOPS provisionadas (SSD).
- El servicio debe permitir ampliar automáticamente el tamaño del volumen de la base de datos a medida que las necesidades de almacenamiento de la base de datos crecen, hasta un máximo de 64 TB o la cantidad máxima que establezca.
- El servicio debe permitir hacer copias de seguridad automatizadas.
- El servicio debe permitir especificar el periodo de retención de copia de seguridad automática hasta un mínimo de 30 días calendario culminados los 12 meses del servicio.
- El servicio debe permitir crear instantáneas de base de datos (copias de seguridad) que inicia el usuario de la instancia almacenada en el servicio de almacenamiento de objetos, y que se conservarán hasta que se eliminen explícitamente.
- El servicio debe soportar la capacidad de notificar eventos de la base de datos por email o SMS.
- El servicio debe contar con capacidad de conmutación por error (automatizada)
- El servicio debe contar con capacidad de prueba de conmutación por error (manual).

4.1.5 Servicios de Red de entrega de contenido:

- Distribuir Aplicaciones, Datos, videos, archivos estáticos y APIs de usuarios de todo el mundo de forma segura.
- Baja latencia de exposición de contenido.
- Altas velocidades de transferencia.
- Capacidades de seguridad avanzada como cifrado completo y compatibilidad con HTTPS.
- Integración con otros servicios de firewall, ruteo, gestión de dominios, etc.
- Protección contra ataques DDoS a las capas de aplicación y red.
- Servicio con ubicaciones de red de bordes, con escalado de manera global y conectados a la red Cloud.
- Mejorar la experiencia de usuario, más segura, de mayor rendimiento y disponibilidad.

4.1.6 Servicio de direccionamiento IP público

- El servicio debe permitir asignar direcciones IP públicas únicas para habilitar la comunicación entre recursos internos y redes externas a través de Internet.
- El servicio debe ofrecer direcciones IP que se puedan asociar de forma dinámica a instancias o recursos de red, permitiendo su reasignación sin necesidad de reiniciar los servicios.

- El servicio debe permitir la reserva de direcciones IP públicas persistentes que no cambien ante reinicios o detenciones del recurso asociado.
- El servicio debe facilitar la gestión centralizada y automatizada de direcciones IP mediante API o consola de administración.
- El servicio debe soportar la asociación de direcciones IP con interfaces de red virtuales en entornos multizona y altamente disponibles.
- El servicio debe incluir funciones para liberar, reasignar o mover direcciones IP de forma segura entre recursos en la infraestructura.

4.1.7 Servicio de gestión de secretos

- El servicio debe ofrecer una plataforma como servicio (PaaS) para la gestión segura de credenciales, claves de acceso, tokens y otros secretos sensibles, permitiendo la administración centralizada, el acceso seguro y la rotación automatizada sin necesidad de administrar infraestructura subyacente.
- El servicio debe permitir almacenar, gestionar y recuperar de manera segura credenciales, claves API, contraseñas, tokens de acceso y otros secretos.
- Debe cifrar automáticamente todos los secretos almacenados con un mecanismo de cifrado seguro administrado por el proveedor.
- Debe soportar políticas de acceso basadas en permisos y roles para restringir el acceso a los secretos según perfiles definidos.
- El servicio debe soportar rotación automática de secretos sin impacto en la disponibilidad de las aplicaciones que los utilizan.
- Debe permitir definir políticas de rotación personalizadas, estableciendo intervalos de tiempo específicos o eventos de seguridad que activen la rotación.
- Debe integrarse con servicios de bases de datos relacionales, almacenamiento de objetos, sistemas de autenticación y otras aplicaciones para actualizar automáticamente los secretos en los sistemas correspondientes.
- Debe permitir la recuperación segura de secretos a través de SDKs, API REST y herramientas de línea de comandos.
- Debe permitir auditar el historial de versiones de cada secreto, asegurando trazabilidad en los cambios realizados.

4.1.8 Servicio de Firewall de aplicaciones web:

- El servicio debe permitir crear reglas para filtrar el tráfico web en función de condiciones como la dirección IP, los encabezados y cuerpos HTTP o los URI personalizados.
- El servicio debe permitir crear reglas que bloqueen ataques comunes como la inyección SQL o el scripting entre sitios.
- El servicio debe permitir crear un conjunto centralizado de reglas que puede implementar en varios sitios web.
- El servicio deberá poderse administrar por completo mediante API o soportar RESTful API para gestión de la configuración.
- El servicio debe poderse implementar y aprovisionarse automáticamente con plantillas de muestra que permiten describir todas las reglas de seguridad que la Entidad quiere implementar para sus aplicaciones web.
- El servicio debe proporcionar métricas en tiempo real y registrar solicitudes sin procesar que incluyen detalles sobre direcciones IP, geolocalización, URI, agentes de usuario.
- El servicio debe permitir agregar una lista de IP anónimas para las reglas administradas de la nube.
- El servicio debe permitir una rápida propagación de las reglas definidas.
- El servicio debe contar con protección de bot.
- El servicio debe tener una disponibilidad mínima de 99.95%

4.1.9 Servicio de transferencia de datos:

- El servicio debe permitir la transferencia de datos hacia y desde la infraestructura de proveedor cloud de manera eficiente y segura.
- Debe proporcionar opciones para la transferencia de datos a través de Internet y conexiones directas dedicadas.
- El servicio debe admitir la transferencia de datos en diferentes formatos, incluidos archivos, bases de datos y transmisiones en tiempo real.
- Debe ofrecer opciones de compresión y cifrado para garantizar la seguridad y la eficiencia de la transferencia de datos.
- El servicio debe ser compatible con la migración de datos hacia y desde otros proveedores de servicios en la nube y entornos locales.
- Debe proporcionar herramientas y recursos para supervisar y gestionar la transferencia de datos, incluida la optimización de la velocidad y el rendimiento.
- El servicio debe ser compatible con las políticas de seguridad de la organización, incluida la gestión de acceso y permisos.
- Debe ser facturado según el volumen de datos transferidos y la velocidad de transferencia de datos.

4.1.10 Servicios de Monitoreo y observabilidad:

- El servicio debe permitir monitorear recursos de infraestructura locales, híbridos y de la nube.
- El servicio debe permitir recopilar y obtener acceso a todos los datos de rendimiento y operaciones en formato de registros y métricas a partir de una sola plataforma.
- El servicio debe permitir visualizar y analizar el estado, el rendimiento y la disponibilidad de sus aplicaciones en un solo lugar.
- El servicio debe tener la capacidad de hacer monitoreo de las aplicaciones en tres dimensiones: monitoreo de infraestructura (con métricas y registros para comprender los recursos que respaldan sus aplicaciones), monitoreo de transacciones (con rastreos para comprender las dependencias entre sus recursos) y monitoreo de usuario final (para monitorear sus puntos de enlace y notificarle cuando su experiencia de usuario final se haya degradado).
- El servicio debe permitir monitorear puntos de enlace de la aplicación.
- El servicio debe permitir escribir reglas para indicar los eventos de interés para la aplicación y las acciones automatizadas que se deben desencadenar cuando una regla concuerde con un evento.
- El servicio debe facilitar el diagnóstico, aislamiento y corrección de problemas
- El servicio debe permitir realizar análisis históricos para optimizar costos y obtener información en tiempo real sobre los recursos de la infraestructura y la optimización de las aplicaciones.
- El servicio debe permitir recopilar hasta 50 métricas predeterminadas de servicios de la nube.
- El servicio debe permitir crear gráficos reutilizables y ver las aplicaciones y los recursos de la nube en una vista unificada.
- El servicio debe permitir monitorear contenedores.
- El servicio debe contar con granularidad configurable de monitoreo/alerta.
- El servicio debe permitir correlacionar el patrón de registros de una métrica específica y definir alarmas para que avisen de manera proactiva acerca de problemas operativos y de rendimiento.
- La funcionalidad de alarmas debe permitir definir un umbral de métricas y activar una acción.
- El servicio debe permitir monitorear el rendimiento operativo, resolver errores y detectar tendencias
- El servicio debe permitir controlar qué usuarios y recursos tienen permiso para obtener acceso a sus datos y de qué manera lo hacen

- El servicio debe permitir cifrar los datos en tránsito y en reposo.

4.1.11 Servicios de respaldo:

- El servicio debe brindar acceso a una consola centralizada de copias de seguridad.
- El servicio debe permitir administrar de manera centralizada políticas de copias de seguridad que cumplan con sus requisitos pertinentes y aplicarlas en recursos de la nube.
- El servicio debe permitir definir políticas de retención de copias de seguridad automáticamente de acuerdo con los requisitos de la Entidad y de conformidad normativa vinculados con el respaldo.
- El servicio debe permitir almacenar las copias de seguridad periódicas de una manera gradual y eficiente.
- Debe permitir los respaldos basados en snapshots.

4.1.12 Servicios de gestión de DNS:

- El servicio debe contar con alta disponibilidad (mínimo 99.9%) y capacidad de escalamiento según demanda.
- El servicio debe permitir crear reglas de reenvío condicional y puntos de enlace DNS para resolver nombres personalizados controlados en las zonas privadas alojadas en el servicio o en los servidores DNS que se encuentran en las instalaciones.
- El servicio debe permitir redirigir a los usuarios finales hacia los mejores puntos de enlace para la aplicación en función de la geo-proximidad, la latencia, el estado y otras consideraciones.
- El servicio debe permitir remitir a los usuarios finales a un punto de enlace determinado que la Entidad especifique en función de la ubicación geográfica del usuario final.
- El servicio debe permitir administrar nombres de dominio personalizados para los recursos de la nube internos sin exponer datos de DNS en la web pública.
- El servicio debe permitir dirigir automáticamente a los visitantes del sitio web a una ubicación alternativa para evitar interrupciones del servicio.
- El servicio debe permitir dirigir automáticamente a los visitantes del sitio web a una ubicación alternativa para evitar interrupciones del servicio.
- El servicio debe ofrecer servicios de registro de nombres de dominio, donde sea posible buscar y registrar nombres de dominio disponibles o transferir nombres de dominio existentes para que se administren a través del servicio.
- El servicio debe contar con una sencilla interfaz de servicios web que permita ponerse en marcha en cuestión de minutos.
- El servicio debe permitir transferir el dominio desde otro servicio DNS al servicio DNS en la nube.
- El servicio debe ofrecer un conjunto sencillo de API que facilita la creación y la administración de registros DNS para los dominios
- El servicio debe incluir la funcionalidad de administración de nombres DNS para escalar hacia arriba o hacia abajo el microservicio.
- El servicio debe tener una disponibilidad del 99.9% como mínimo.

4.2 Infraestructura de la nube requerida

La solución de nube pública a contratar deberá contemplar los recursos mínimos detallados a continuación, los cuales permitirán garantizar la operación, escalabilidad y seguridad del Sistema de Trámite Documentario institucional, así como el desarrollo e implementación de nuevas aplicaciones digitales del OEDI.

Todos los recursos deberán ser configurables, escalables y administrables desde la consola central del servicio de nube pública contratado.

El presente servicio incluye:

Componente del Servicio	Subcomponente / Descripción	Especificación	Cantidad Mensual Mínima
Servicios de cómputo de instancias virtuales	Sistema operativo	Linux	1
	vCPU	2	
	Memoria RAM	16 GB	
	Disco SSD	140 GB	
	Velocidad de Reloj	2.2 GHz	
Servicios de cómputo de instancias virtuales	Sistema operativo	Linux	1
	vCPU	2	
	Memoria RAM	8 GB	
	Disco SSD	30 GB	
	Velocidad de Reloj	2.2 GHz	
Servicios de cómputo de instancias virtuales	Sistema operativo	Windows Server 2025	1
	vCPU	4	
	Memoria RAM	16 GB	
	Disco SSD	100 GB	
	Velocidad de Reloj	3.6 GHz	
Servicio de bases de datos relacionales (PostgreSQL)	Motor	Postgres	4
	vCPU	2	
	RAM	16 GB	
	SSD	100 GB	
Servicio de bases de datos relacionales (PostgreSQL)	Motor	Postgres	1
	vCPU	2	
	RAM	16 GB	
	SSD	30 GB	
Servicio de red de entrega de contenido (CDN)	Transferencia de datos salientes (GB)	100	1
	Número de consultas (M)	6	
Servicio de direccionamiento IP público	Cantidad de IPs públicas	4	1
Servicio de gestión de secretos	Secretos	2	1
	Llamadas a la API	2000	
Servicio de Firewall de Aplicaciones Web (WAF)	Web ACL	2	1
	Número de consultas	6 M	
	Reglas	10	

Servicio de transferencia de datos	Transferencia de datos salientes (GB)	300	1
Servicio de monitoreo y observabilidad	Paneles	2	1
	Datos de registros ingeridos (GB)	20	
	Datos de logs escaneados (GB)	200	
	Alarmas	15	
Servicio de respaldos	Frecuencia	Diaria	1
	Retención	14 días	
	Recursos	MVs, BDs (ver leyenda)	
	Cambio diario estimado	0.50%	
Servicio de gestión de DNS	Cantidad zonas hosteadas	2	1

Leyenda Nomenclaturas:
vCPU = Unidad virtual de procesamiento. Equivale a un núcleo lógico de CPU.
GB = Gigabyte. Unidad de medida de almacenamiento o memoria.
M = Millones.
MVs = Máquinas Virtuales incluidas en el servicio (todas las instancias de cómputo listadas).
BDs = Bases de datos incluidas en el servicio (todas las instancias de base de datos listadas).
Web ACL = Lista de control de acceso web utilizada por el firewall de aplicaciones web para permitir o bloquear tráfico según reglas definidas.

4.3 Plan de Trabajo

El proveedor deberá presentar, dentro de los tres (03) días calendario, desde el día siguiente de la notificación de la orden de servicio, un Plan de Trabajo integral a través de la Mesa de Partes Virtual de la Entidad (https://sgd.oedi.gob.pe/mpvdoc/inicio.do), el cual deberá incluir:

- Cronograma con fases bien definidas (planificación, diseño, ejecución, validación, transición).
- Matriz de responsabilidades (RACI).
- Cronograma con tareas y subtareas desglosadas.

4.3.1. Implementación de la solución:

- **Se realizará la configuración avanzada de la infraestructura en la nube pública, contemplando:**
- Separación de entornos: pruebas, producción.
- Segmentación de redes virtuales por ambiente y aplicación.
- Implementación de políticas de control de acceso, auditoría de acciones y gestión de identidades con autenticación multifactor.
- Definición de etiquetas de control de costos por recurso y área funcional.

- **Se ejecutará una migración planificada de la base de datos (versión 16.6), que incluirá:**

- Análisis previo de la estructura, tamaño y consistencia de datos.
- Refactorización o adecuación de elementos que presenten incompatibilidades.
- Migración en fases, según ventanas de mantenimiento definidas, con validación de integridad y pruebas de consistencia post migración.

- **Se configurará una red de entrega de contenidos (CDN) que contemple:**
- Políticas diferenciadas de caché por tipo de contenido (archivos estáticos, multimedia, API).
- Integración con reglas de seguridad que incluyan redirección segura (HTTPS), encabezados de política de contenido y autenticación basada en tokens.

- **Se implementará un firewall de aplicaciones web con:**
- Reglas administradas y personalizadas para distintos tipos de tráfico.
- Control geográfico, validación de solicitudes, y protección contra bots automatizados.
- Registro detallado de eventos con integración a paneles de monitoreo y alertas.

- **Se habilitará una estrategia de respaldos multinivel, incluyendo:**
- Respaldos automáticos diarios con política de retención de 14 días.
- Snapshots antes de actividades críticas.
- Versionado de archivos y datos en repositorio seguro.
- Validación periódica de capacidad de restauración.

- **Se ejecutarán pruebas exhaustivas sobre la solución desplegada:**

- Pruebas funcionales: validación del correcto funcionamiento de los componentes y servicios implementados.
- Pruebas de carga: verificación del comportamiento del sistema bajo distintos niveles de concurrencia y estrés.

- **Validación de entorno de pruebas:**
- Toda la implementación deberá realizarse previamente en un entorno de pruebas replicado, que permita validar el comportamiento integral de los sistemas antes del pase a producción.

- **Automatización de la Infraestructura:**
- Se deberá desarrollar la automatización de la infraestructura mediante código, utilizando herramientas declarativas de infraestructura como código (IaC), integradas con versiones controladas y documentadas.

El plazo de implementación del servicio será realizado en un plazo máximo de cinco (5) días calendario, contados a partir del día siguiente de presentado el plan de trabajo. Culminado la implementación se suscribirá un acta de inicio de la prestación del servicio.

4.3.2 Soporte

El contratista deberá proveer un servicio de soporte técnico integral y especializado bajo las siguientes características mínimas:

- **Cobertura:**
- El soporte deberá brindarse en modalidad **24 horas al día**, **7 días a la semana, los 365 días del año (24x7x365)**, e incluirá asistencia técnica, informática y operativa para todos los niveles de soporte requeridos.
- Este servicio de soporte estará incluido en el contrato, sin costos adicionales para la Entidad.
- **Canales de atención:**

- **Telefónico**: a través de un número de contacto (fijo o móvil) disponible 24x7, destinado a la atención de cualquier tipo de incidente, requerimiento o consulta.
- **Correo electrónico**: mediante una cuenta exclusiva asignada para la gestión de solicitudes.
- **Web o chat:** el proveedor podrá habilitar atención via portal web o chat en línea; estos canales deberán ser confirmados y oficializados por escrito al inicio del servicio.
- **Soporte remoto:**
- El proveedor y su personal a cargo deben brindar soporte remoto, cuando se requiera.
- El contratista debe designar a un responsable y señalar por escrito los datos de contacto de éste para la atención de los inconvenientes, reclamos, gestionar los pedidos, entre otros.
- En caso de existir modificaciones en los contactos, éstas deberán ser informadas y remitidas por la Mesa de Partes.

El proveedor como parte del soporte deberá entregar un (1) informe mensual, por un total de doce (12) informes, con el siguiente contenido mínimo:

- El proveedor deberá presentar un reporte de rendimiento de la infraestructura de los últimos 30 días, donde considere métricas como CPU, RAM, DISCO, RED.
- El proveedor deberá presentar un registro con las incidencias reportadas por la Entidad durante el mes.
- El proveedor deberá presentar un reporte detallado de las incidencias de seguridad detectadas o gestionadas durante el periodo, incluyendo: descripción del incidente, fecha y hora de ocurrencia, impacto, acciones correctivas y medidas preventivas implementadas.
- Recomendaciones y/o sugerencias.

Cada informe debe ser entregado en los primeros diez (10) días calendario del mes siguiente al periodo mensual transcurrido mediante la Mesa de Partes Virtual (https://sgd.oedi.gob.pe/mpvdoc/inicio.do) o Física de la Entidad.

4.3.3 Atención de Requerimientos

El contratista deberá implementar un procedimiento formal para la atención y gestión de requerimientos que puedan surgir durante la vigencia del contrato, bajo las siguientes condiciones:

Tipos de requerimientos:

- Incidentes técnicos que afecten la disponibilidad, seguridad o rendimiento del servicio.
- Requerimiento de cambios de configuración o ajustes en la infraestructura, incluyendo aquellos que implique gestión de cambios.
- Consultas técnicas o solicitudes de información relacionadas con la operación del servicio.
- Solicitudes de restauración de respaldo o de acceso a registros históricos de monitoreo.

Requerimientos que implican gestión de cambios: Se entenderá como gestión de cambios toda solicitud que:

- Debe ser ejecutada exclusivamente por personal con perfil de especialista cloud.
- Requiera modificación de la configuración central de la infraestructura, políticas de acceso, reglas de firewall, base de datos, monitoreo u otros componentes críticos del servicio.

Tiempo de Respuesta para Requerimientos

Se define como tiempo de respuesta para requerimientos al tiempo transcurrido desde el momento en que la Entidad realiza un pedido al contratista y el momento en que el requerimiento ha sido recibido. Luego el personal especializado se comunicará con la Entidad para informar que el requerimiento ha sido recibido para su pronta atención.

Tiempo de respuesta: 2 horas en 8x5.

Característica	Descripción
Horario de Atención (No incluye días festivos ni feriados)	Los horarios de atención solicitados son: Gestión de Requerimientos 8:30 am a 6:00 pm (L-V)

4.3.4 Atención de Incidencias

El tiempo de respuesta ante una incidencia, se define como el tiempo transcurrido entre el momento en que la Entidad notifica la avería o si la avería es detectada internamente por el proveedor y el momento en que un técnico del servicio empieza a trabajar en la resolución del problema y además se realiza la primera comunicación con la Entidad.

Cada incidencia estará asociada a un nivel de severidad descrito a continuación:

Severidad	Descripción	Tiempos de respuesta
Nivel 1 (Graves)	Fallos que involucran una indisponibilidad del servicio de infraestructura cloud.	30 minutos en 7x24
Nivel 2 (Medias)	Fallos que involucran una degradación en la calidad del servicio, tal como la saturación de recursos, atención de servicios a una capacidad menor al 100%.	1 hora en 7x24
Nivel 3 (Leves)	Fallos que involucran a funcionalidades secundarias del servicio y que no afectan su normal operatividad.	2 horas en 8x5 y 4 horas en 7x24

Los niveles de severidad servirán a los grupos de operación para priorizar las incidencias y atenderlas en base a los tiempos de respuesta.

Característica	Descripción
Horario de Atención (De acuerdo con el nivel de severidad, se debe atender en 7x24 (L-D) u 8x5(L-V)	Los horarios de atención solicitados son: Gestión de Incidentes 24 x 7 x 365 (*)

4.4. Sistema de entrega para bienes y servicios

4.4.1 Diseño y operación y mantenimiento

No corresponde.

4.4.2 Gestión de 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

4.8. Lugar y plazo de prestación del servicio

- **Lugar**

La implementación del servicio podrá realizarse de manera presencial en las instalaciones ubicadas en **Av. Javier Prado Oeste N.º 2801 – San Isidro, Provincia y Departamento de Lima**, o de forma remota, según las coordinaciones que se efectúen con el equipo designado del OEDI.

- **Plazo de prestación del servicio**

El plazo de servicio será de trescientos sesenta y cinco (365) días calendario, contados a partir del día siguiente a la firma del 'Acta de inicio de la prestación del servicio'.

4.9 Entregable

Deberá presentar la documentación siguiente:

- Informe de implementación del servicio, que deberá contener como mínimo lo siguiente
  - Diseño de la solución, detallando componentes, flujos de datos, capacidades asignadas y dependencias
  - Evidencia de la implementación realizada.
  - Pruebas técnicas realizadas
  - Niveles de escalamiento
  - Credencial de acceso a herramientas y recursos para supervisar y gestionar la transferencia de datos, incluida la optimización de la velocidad y el rendimiento.

El informe deberá ser presentado en un plazo máximo de hasta 05 días calendario posteriores a la suscripción del acta del Acta de inicio de prestación del servicio.

- 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

5.1. 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.
- El postor deberá presentar carta y/o certificado de respaldo como partner avanzado oficial de la marca (fabricante) de la nube pública a ofertar o similar.
- Código de cuenta interbancario (CCI).
- Persona natural y/o jurídica.
- No debe tener impedimentos para contratar con el Estado.

- De acuerdo a los lineamientos para el uso de servicios en la nube para entidades de la administración pública del estado peruano, se requiere que el proveedor de servicios en la nube cuente como mínimo con un certificado de seguridad de la información ampliamente reconocido y basado en estándares internacionales, tales como ISO/IEC 27001 o ISO/IEC 27017 o ISO/IEC 27018.

5.2. Requisitos del proveedor

El postor debe acreditar un monto facturado acumulado equivalente a **S/ 60,000.00 (sesenta mil con 00/100 soles)**, por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los quince años anteriores a la fecha de la presentación de ofertas que se computa 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 contratación de servicios iguales o similares al objeto de la convocatoria, durante los quince años anteriores a la fecha de la presentación de ofertas que se computa desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda

Se consideran servicios similares a los siguientes: implementación de proyectos de nubes públicas y/o Servicios Cloud Computing y/o Servicios de Informática en la Nube y/o Cloud web Hosting y/o Servicio de infraestructura en nube y/o servicio administrado de infraestructura en nube.

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 constancia 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[1], o comprobantes de retención electrónico emitido por SUNAT por la retención del IGV[2], correspondientes a un máximo de veinte (20) contrataciones. En caso el postor sustente su experiencia en la especialidad mediante contrataciones realizadas con privados[3], para acreditarla debe presentar de forma obligatoria lo indicado en el numeral (ii) del presente párrafo; no es posible que acredite su experiencia únicamente con la presentación de contratos u órdenes de compra con conformidad o constancia de prestación.

5.3. Equipamiento

[1] El solo sello de cancelado en el comprobante de pago, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Es válido el sello colocado por el cliente del postor (sea utilizando el término "cancelado" o "pagado").

[2] De acuerdo con el Régimen de Retenciones del Impuesto General a las Ventas (IGV).

[3] Se entiende "privados" como aquellos que no son entidades contratantes.

5.3.1. Equipamiento estratégico

No corresponde

5.3.2. Equipamiento no estratégico

No corresponde

5.4. Infraestructura estratégica

No corresponde

5.5. Personal

Personal: Jefe de Proyecto

5.5.1 Actividades

- Estará a cargo de la dirección general del proyecto, será el encargado de efectuar las coordinaciones directas con el Coordinador de TI o quien haga sus veces del Organismo de Estudios y Diseño de Proyectos de Inversión (OEDI) durante la etapa de la implementación.
- Realizará las coordinaciones con el personal del Organismo de Estudios y Diseño de Proyectos de Inversión (OEDI)
- Informará sobre el avance de la implementación.
- Elaborará las actas de reunión de trabajo.
- Gestionará las pruebas de validación para el acta de conformidad
- Coordinar con los implementadores el cumplimiento de los objetivos en el tiempo planificado.
- Reportar los avances según el cronograma establecido en el plan de trabajo
- Generar la documentación respectiva.

5.5.2 Formación académica:

Profesional titulado o Bachiller en las siguientes carreras: Ingeniería de Software o Ingeniería de Redes y Comunicaciones o Ingeniería de Sistemas de Información o Ingeniería de Computación y de Sistemas.

Acreditación:

El GRADO O TÍTULO PROFESIONAL será verificado por la DEC en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: *https://enlinea.sunedu.gob.pe/* o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: *https://titulosinstitutos.minedu.gob.pe/*, según corresponda.

El postor debe señalar los nombres y apellidos, DNI y profesión del personal clave, así como el nombre de la universidad o institución educativa que expidió el grado o título profesional requerido.

En caso EL GRADO O TÍTULO PROFESIONAL no se encuentre inscrito en los referidos registros, el proveedor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.

5.5.3. Experiencia:

Deberá acreditar experiencia mínima de 3 años, desempeñándose como gerente, gestor, jefe, responsable o líder de proyectos en servicios en la nube o en tecnologías de la información.

Acreditación:

La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: **(i)** copia simple de contrato u orden de servicio 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.

5.5.4 Certificación:

- Certificación de Gestión de Proyectos PMP vigente y/o certificado SCRUM Master
- Certificado de ITIL Foundation Certificate.

Acreditación:

- **Se acreditará con copia simple de la certificación, el cual deberá estar vigente a la fecha de presentación de oferta.**

Personal: Especialista implementador.

5.5.5 Actividades

- Realizará las coordinaciones con el personal del Organismo de Estudios y Diseño de Proyectos de Inversión (OEDI) Responsable de las arquitecturas de la solución.
- Desarrollará toda la infraestructura como código (IaC) para la homologación de los ambientes en nube pública.
- Realizará los planes de recuperación ante desastres para las arquitecturas a implementar.
- Evaluar continuamente las arquitecturas existentes para identificar áreas de mejora o potenciales cuellos de botella.
- Asegurar que todas las soluciones cumplan con los estándares de seguridad necesarios y recomendar soluciones de seguridad adecuadas.
- Participar en reuniones estratégicas para ofrecer aportaciones desde la perspectiva de la nube pública y cómo puede influir en la dirección futura de la empresa.
- Documentar todas las arquitecturas y soluciones implementadas de manera clara y concisa para futuras referencias o para nuevos miembros del equipo.

5.5.6 Formación académica:

Profesional titulado o Bachiller en las siguientes carreras: Ingeniería de Software o Ingeniería de Redes y Comunicaciones o Ingeniería de Sistemas o Ingeniería de Sistemas de Información o Ingeniería Informática o a fines.

Acreditación:

El **grado o título profesional** requerido, será verificado en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria – SUNEDU o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación, según corresponda.

En caso el **grado o título profesional** requerido no se encuentre inscrito en el referido registro, el proveedor/postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.

5.5.7. Experiencia:

Deberá acreditar experiencia mínima de 3 años en desarrollo y/o arquitectura y/o implementación y/o configuración y/o instalación de soluciones en nube pública o soluciones de cloud o soluciones de cloud computing o infraestructura en nube pública.

Acreditación:

La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: **(i)** copia simple de contrato u orden de servicio 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.

5.5.8 Certificación:

- Certificado oficial en arquitectura cloud de nivel profesional de la marca de la nube pública a ofertar.

Acreditación:

Se acreditará con copia simple de la certificación, el cual deberá estar vigente a la fecha de presentación de oferta.

VI. OTRAS CONSIDERACIONES PARA LA EJECUCIÓN DE LA PRESTACIÓN

6.1 Adelantos

No corresponde.

6.2 Modalidades de pago

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

6.3 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 de la ejecución del presente servicio, elaborado por el Coordinador de Tecnología de la Información o quien haga sus veces. En caso corresponda, dicha conformidad deberá señalar los días de retraso injustificado en las que haya incurrido el contratista, a efectos de que la Dependencia Encargada de las Contrataciones -DEC proceda con la determinación del importe a penalizar.

Asimismo, de manera excepcional, se permitirá que el pago se realice de forma total o parcial al inicio de la vigencia contractual, siempre que dicha modalidad constituya una condición de mercado indispensable para la ejecución de las obligaciones a cargo del proveedor, ya sea para la entrega de bienes o la prestación de servicios. Esta disposición se aplicará conforme a lo establecido en la Ley N.º 32069, Ley General de Contrataciones Públicas, y su Reglamento.

6.4 Forma y requisito 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:

- 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.

6.5 Formula de reajuste

No corresponde

6.6. 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

6.6.1. 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 para plazos menores o iguales a sesenta (60) días

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.
Cuando se llegue a cubrir el monto máximo de la penalidad, equivalente al diez

6.6.2 Otras penalidades aplicables

Aplicación	Formula de Calculo	Procedimiento
Retraso en la presentación del plan de trabajo	3 por ciento de la UIT por día de retraso	Verificación de la constancia de mesa de partes por la presentación del plan de trabajo
Retraso en la implementación del servicio	3 por ciento de la UIT por día de retraso	Verificación del acta de inicio de prestación del servicio

6.7 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.

6.8 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.**

6.10 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.

6.10. 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.

6.11. 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[4] 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, participacionistas, 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[5]. 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[6]. En ningún caso, dichas medias impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar[7]

6.12. 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

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

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.

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.

6.13. 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.

6.1.4. 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.

6.15 Anexos

- No corresponde.

FUNCIONARIO SOLICITANTE	
Apellidos y Nombres:	Pedro Arturo 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: 22.07.2025 10:07:00 -05:00

Firma Electrónica