soporteANEXO N°02: FORMATO DE REQUERIMIENTO DE SERVICIOS – TÉRMINOS DE REFERENCIA

REQUERIMIENTO DE SERVICIOS – TÉRMINOS DE REFERENCIA

1. Datos Generales de la Contratación:

1.1. Denominación de la Contratación	SERVICIO DE INFRAESTRUCTURA EN NUBE PÚBLICA AWS PARA LOS SISTEMAS INFORMÁTICOS DE LA ENTIDAD
1.2. Área Usuaria (Unidad Orgánica)	Oficina de Tecnologías de la Información
1.3. Meta Presupuestaria	0025
1.4. Actividad del POI	AOI00163000013- INFRAESTRUCTURA PARA EL DESARROLLO DE APLICACIONES
1.5. Persona responsable del requerimiento su supervisión y seguimiento	Jefe de la Oficina de Tecnologías de la Información
1.6. Persona que otorgará la Conformidad	Jefe de la Oficina de Tecnologías de la Información

2. Finalidad Pública

Fomentar, expandir y ejecutar la investigación científica y tecnológica en el ámbito de los glaciares y Ecosistemas de Montaña; donde se realizan investigaciones y acciones administrativas a través de la renovación de la infraestructura en la nube.

3. Antecedentes:

Desde la creación del INAIGEM a fines del año 2014 y su puesta en marcha en noviembre del 2015, se viene implementando sistemas de información en el INAIGEM, en el 2020 se implementó en la nube el (MGD) Modelo de Gestión Documental que contiene el Sistema de Gestión Documental de acuerdo Decreto Legislativo N° 1310 y otros sistemas de la entidad, actualmente se necesita adquirir el servicio en nube, para lo cual es necesario contar con capacidades dinámicas que pueden ser asignadas de acuerdo a las necesidades requeridas por las aplicaciones antes mencionadas. En este sentido, es importante contar con las capacidades de una infraestructura y servicios en la nube para habilitar las aplicaciones y brindar la atención a los órganos de apoyo, línea y público en general a nivel nacional.

4. Objetivos de la Contratación

4.1. Objetivo General:

El objetivo principal es modernizar la infraestructura de alojamiento de INAIGEM, manteniendo, migrando y alojando todos los sistemas relevantes en la nube de Amazon

Web Services (AWS). Este esfuerzo está en línea con la Resolución de Gerencia General N.° 015-2025-INAIGEM/GG de fecha 5 de marzo de 2025, que establece la Estandarización para la contratación de infraestructura tecnológica en nube Amazon Web Services (AWS) para el servicio de infraestructura en nube para los sistemas informáticos de la entidad por un periodo de sesenta (60) meses.

4.2. Objetivo(s) Específico(s):

- ✔ Contar con servicios de nube de gestión de aprovisionamiento de capacidades de procesamiento, memoria, almacenamiento y redes en modalidad de pago fijo de recursos.
- ✔ Mantener los servidores y sistemas existentes en nube de INAIGEM, en el caso se requiera realizar la migración de la infraestructura on-premise a AWS, se debe seguir las directrices de la Oficina de Tecnologías de la Información.
- ✔ Mantener altos estándares de seguridad y protección de datos, particularmente en lo que respecta a la información crítica manejada por la institución.

5. Sistema de Contratación

El sistema de contratación de la provisión del servicio es de Suma Alzada, bajo la modalidad de ejecución ¨llave en mano¨.

6. Características y condiciones del servicio a contratar

El alcance de la adquisición comprende la entrega de todos los servicios requeridos, acondicionamiento, instalación, configuración, pruebas de funcionalidad y puesta en operación para el correcto funcionamiento.

El presente servicio incluye:

Ítem	Producto	Cantidad
1	Servicio de implementación	01
2	Servicio de infraestructura en nube pública	01
3	Servicio de Gestión y Soporte	01

6.1. Descripción y cantidad del servicio a contratar

Descripción	Cantidad	Unidad de Medida
SERVICIO DE INFRAESTRUCTURA EN NUBE PARA LOS SISTEMAS INFORMÁTICOS DE LA ENTIDAD • La Infraestructura de Nube Pública descrita en los presentes términos de referencia deberá tener una	1	Servicio

disponibilidad mínima del 99.9% en las capacidades de cómputo y 99.5% en base de datos. ● El servicio deberá contar con una plataforma o consola la cual permita administrar los servicios de Infraestructura pública o Nube pública de Microservicios, la misma que será manejado por el Especialista (asignado por la Oficina de Tecnologías de la Información) del Servicio a contratar. ● Asegurar la resiliencia y continuidad del servicio a través de la implementación de como mínimo **dos (2) centros de datos (zonas de disponibilidad) en una misma zona geográfica (región)** que permitan la redundancia y failover automático en caso de incidencias, garantizando así la disponibilidad y la recuperación ante desastres de las aplicaciones y datos de INAIGEM. El servicio de nube pública que ofrecerá el Proveedor deberá contar con las siguientes características: ● El servicio de nube pública 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 vigente. ● El servicio de nube pública debe contar con el catálogo de sus servicios en su respectiva página web, permitiendo que cualquier persona con acceso a internet acceda fácilmente a la descripción de las características técnicas de cada uno de ellos. ● El servicio de nube pública debe ofrecer una calculadora de precios, con la cual el interesado puede proyectar presupuestos. ● El servicio de nube pública debe contar con certificaciones como: a) Cloud Security Alliance (CSA): Controles de la alianza de seguridad en la nube b) FedRAMP c) SOC 1: Informe de controles de auditoría d) SOC 2: Informe de seguridad, disponibilidad y confidencialidad e) SOC 3: Informe de controles generales f) ISO 9001: Estándar de calidad internacional g) ISO 27001: Controles de administración de seguridad h) ISO 27017: Controles específicos de la nube i) ISO 27018: Protección de datos personales j) ISO 22301:2019: Estándar de Sistema de Continuidad de Negocio (BCMS). *Estas certificaciones deben presentar en el entregable de implementación.*		

Av, Centenario 2656 - Sector Palmira- Independencia Huaraz-Ancash - Perú
Av. Antonio Miró Quesada 457 - Oficina 401 Edificio Corporativo ABC LIma - LIma - Magdalena del Mar - Perú
Av. Industrial Nro. Mz. N Lt 1 Urb. Residencial Huancaro - Santiago - Cusco - Perú

6.1.1 Componentes del servicio

El INAIGEM requiere contratar un Servicio de Infraestructura (IaaS) y alojamiento en la nube de las aplicaciones de la institución por un periodo mínimo de doce (12) meses o hasta agotar los créditos que le permita tener escalabilidad y disponibilidad (para crecer en recursos de almacenamiento, procesamiento y memoria), y afrontar de esta forma, todos los escenarios futuros posibles.
Las aplicaciones de la institución a migrar y/o mantener tanto en cloud como en on-premise incluyen:

CLOUD

- api-convocatorias.inaigem.gob.pe
- api-monfu.inaigem.gob.pe
- api-politicas.inaigem.gob.pe
- api-register.inaigem.gob.pe
- api-seguimiento.inaigem.gob.pe
- api-seguimiento-sgd.inaigem.gob.pe
- buscador-convenios.inaigem.gob.pe
- consultaexpediente.inaigem.gob.pe
- convenios.inaigem.gob.pe
- convocatorias.inaigem.gob.pe
- correo.inaigem.gob.pe
- cris.inaigem.gob.pe
- dashboard.inaigem.gob.pe
- datacocha.inaigem.gob.pe
- datacochageoespacial.inaigem.gob.pe
- geoportal.inaigem.gob.pe
- guard.inaigem.gob.pe
- intranet.inaigem.gob.pe
- manuales.bitacora.inaigem.gob.pe
- manuales.inaigem.gob.pe
- manuales.mpve.inaigem.gob.pe
- manuales.sgp.inaigem.gob.pe
- mpve.inaigem.gob.pe
- mpveapi.inaigem.gob.pe
- permafrost.inaigem.gob.pe
- perugrows.inaigem.gob.pe
- politica.inaigem.gob.pe
- puyaraimondii.inaigem.gob.pe
- registro-asistencia.inaigem.gob.pe
- repositorio.inaigem.gob.pe
- rrhh.inaigem.gob.pe
- seguimiento.inaigem.gob.pe

Av, Centenario 2656 - Sector Palmira- Independencia Huaraz-Ancash - Perú
Av. Antonio Miró Quesada 457 - Oficina 401 Edificio Corporativo ABC LIma - LIma - Magdalena del Mar - Perú
Av. Industrial Nro. Mz. N Lt 1 Urb. Residencial Huancaro - Santiago - Cusco - Perú

• sgd.inaigem.gob.pe • sigidi.inaigem.gob.pe • simposio.inaigem.gob.pe • sinoe.inaigem.gob.pe • spring-ianify-api.inaigem.gob.pe • sso.inaigem.gob.pe • videos.bitacora.inaigem.gob.pe • videos.inaigem.gob.pe • videos.mpve.inaigem.gob.pe • visor.inaigem.gob.pe **LOCAL (ON-PREMISES)** • sigaweb.inaigem.gob.pe • sige.inaigem.gob.pe • apiconvenios.inaigem.gob.pe Todas estas aplicaciones deberán mantenerse desplegadas en la infraestructura de nube y local según lo detallado. Se describe la infraestructura en nube desplegada en el ítem 6.2. Requisitos de capacidad. Lo solicitado es en base a lo que se cuenta actualmente y es suficiente para alojar todas las aplicaciones. **De acuerdo con el tiempo de servicio requerido, se recomienda la adopción de Savings Plans para optimizar los costos de los recursos solicitados.** Asimismo, se aclara que el pago bajo esta modalidad es que se realizará el pago del presente servicio en una sola armada. Los componentes con los que debe contar el requerido IaaS, son los siguientes: • **Servicios de gestión de identidad y acceso** a. El servicio debe permitir controlar el acceso, permisos a sus recursos y servicios de la nube. b. El servicio debe permitir que se administren permisos para sus usuarios y aplicaciones. c. El servicio debe permitir usar identidad federada para administrar accesos a una cuenta. d. El servicio debe permitir analizar el acceso a recursos y servicios. e. 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. f. El servicio debe permitir crear credenciales temporales.		

Av, Centenario 2656 - Sector Palmira- Independencia Huaraz-Ancash - Perú
Av. Antonio Miró Quesada 457 - Oficina 401 Edificio Corporativo ABC LIma - LIma - Magdalena del Mar - Perú
Av. Industrial Nro. Mz. N Lt 1 Urb. Residencial Huancaro - Santiago - Cusco - Perú

g. El servicio debe permitir identificar y eliminar fácilmente los permisos no utilizados. h. El servicio debe permitir diferentes modos de autenticación de usuarios como contraseñas, pares de claves y autenticación multifactor i. El servicio debe soportar la federación desde sistemas corporativos como Microsoft Active Directory, así como proveedores de identidad basados en estándares. j. El servicio debe permitir bloquear los puertos que dan acceso a la nube pública y generar listas blancas de direcciones IP a través políticas k. El servicio debe permitir contar con información de auditoría de accesos a los recursos de la nube. ● **Servicios de red** a. El servicio debe ser escalable y debe permitir especificar un rango de direcciones IP privadas de que sean elegidas. b. El servicio debe permitir ampliar la nube privada virtual mediante la incorporación de intervalos IP secundarios. c. El servicio debe permitir dividir el rango privado de direcciones IP privadas de la nube privada virtual en una o varias subredes públicas o privadas para posibilitar la ejecución de aplicaciones y la prestación de servicios en la nube privada virtual. d. El servicio debe permitir controlar el acceso de entrada y salida desde y hacia subredes individuales por medio de listas de control de acceso. e. El servicio debe permitir almacenar datos y definir permisos de forma que el acceso a los datos sea posible exclusivamente desde el interior de la nube privada virtual. f. El servicio debe permitir asignar varias direcciones IP y asociar múltiples interfaces de red elásticas a instancias de la nube privada virtual. g. El servicio debe permitir asociar una o más direcciones IP elásticas a cualquier instancia de la nube privada virtual, de modo que puedan alcanzarse directamente desde Internet. h. El servicio debe permitir conectarse a la nube privada virtual con otras nubes privadas virtuales y obtener acceso a los recursos de otras nubes		

Av, Centenario 2656 - Sector Palmira- Independencia Huaraz-Ancash - Perú
Av. Antonio Miró Quesada 457 - Oficina 401 Edificio Corporativo ABC LIma - LIma - Magdalena del Mar - Perú
Av. Industrial Nro. Mz. N Lt 1 Urb. Residencial Huancaro - Santiago - Cusco - Perú

privadas virtuales a través de direcciones IP privadas mediante la interconexión de nube privada virtual. i. El servicio debe permitir conectarse de manera privada a los servicios del fabricante de la nube pública sin usar una gateway de Internet, ni una NAT ni un proxy de firewall mediante un punto de enlace de la nube privada virtual. j. El servicio debe permitir conectar la nube privada virtual y la infraestructura de TI local con la VPN del fabricante de la nube pública de sitio a sitio. k. El servicio debe permitir asociar grupos de seguridad de la nube privada virtual con instancias en la plataforma. l. El servicio debe permitir registrar información sobre el tráfico de red que entra y sale de las interfaces de red de la nube privada virtual. m. El servicio debe permitir habilitar IPv4 e IPv6 en la nube privada virtual. n. El servicio debe tener la habilidad de mover direcciones entre instancias o. El servicio debe tener la capacidad de análisis para monitoreo de tráfico de red. ● **Servicios de Respaldo** a. El servicio debe brindar acceso a una consola centralizada de copias de seguridad. b. 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. c. 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. d. El servicio debe permitir almacenar las copias de seguridad periódicas de una manera gradual y eficiente. e. Debe permitir los respaldos basados en snapshots. ● **Servicio de Gestión de Certificados Digitales** a. El servicio debe crear, almacenar y renovar certificados y claves SSL/TLS X.509 vigente que protegen sus sitios web y aplicaciones descritas con el proveedor de nube.		

Av, Centenario 2656 - Sector Palmira- Independencia Huaraz-Ancash - Perú
Av. Antonio Miró Quesada 457 - Oficina 401 Edificio Corporativo ABC LIma - LIma - Magdalena del Mar - Perú
Av. Industrial Nro. Mz. N Lt 1 Urb. Residencial Huancaro - Santiago - Cusco - Perú

• **Servicios de cómputo de instancias virtuales** a. 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. b. El servicio debe permitir pausar y reanudar las instancias. c. El servicio debe contar con la capacidad para lanzar / administrar un grupo de recursos de cómputo con una sola solicitud. d. El servicio debe permitir hacer seguimiento de licencias para regular el uso y el cumplimiento. e. El servicio debe permitir implementar funcionalidades de auto escalamiento. f. El servicio debe contar con la capacidad de sincronización de tiempo para instancias cómputo. g. El servicio debe soportar acceso SSH basado en políticas. h. El servicio debe ser suministrado bajo un esquema de pago por uso. i. El servicio debe ofrecer la posibilidad de colocar instancias en distintas regiones de disponibilidad. j. El servicio debe permitir el uso de direcciones IP públicas. k. El servicio debe permitir ajustar la escala de la capacidad de las instancias automáticamente de acuerdo con las condiciones que se definan. l. 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. m. Debe ofrecer un servicio de origen de hora de alta precisión, fiabilidad y disponibilidad que pueda ser usado por los servicios de cómputo. • **Servicios de almacenamiento de datos** a. El servicio debe permitir crear volúmenes de almacenamiento y adjuntarlos a recursos de cómputo. b. El servicio debe permitir crear un sistema de archivos sobre estos volúmenes, ejecutar una		

base de datos o darles cualquier otro uso que le daría al almacenamiento en bloques. c. El servicio debe ofrecer almacenamiento respaldado por SSD para cargas de trabajo transaccionales como bases de datos y volúmenes de arranque (el rendimiento depende principalmente de las IOPS) y almacenamiento respaldado por HDD para cargas de trabajo intensivas como el procesamiento de registros (el rendimiento depende principalmente de los MB/s). d. El servicio debe permitir aumentar la capacidad, ajustar el rendimiento y modificar el tipo de cualquier volumen de generación nueva o existente de manera dinámica. e. El servicio debe estar diseñado para ofrecer una alta disponibilidad y fiabilidad a través de la duplicación en múltiples ubicaciones. f. El servicio debe permitir hacer un cifrado integral de las instantáneas, los volúmenes de arranque y los volúmenes de datos. g. El servicio debe soportar la generación de Backup sin interrupción del servicio. h. El servicio debe contar con rendimiento total predecible del volumen creado a partir de instantáneas ● **Servicios de Base de datos relacional** a. 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 cual será realizado por el proveedor. b. El servicio debe ofrecer varios tipos de recursos de cómputo: optimizados para memoria, rendimiento u operaciones de E/S c. El servicio debe permitir escoger entre los siguientes motores de bases de datos PostgreSQL, MSSQL y MySQL d. El servicio debe permitir utilizar el licenciamiento de la base de datos Oracle bajo el modelo “Bring Your Own license” e. 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.		

f. El servicio se debe poder desplegar en múltiples ubicaciones. g. El servicio debe permitir aplicar de forma automática parches de software. h. El servicio debe contar con la opción de controlar si se deben aplicar parches a un recurso de cómputo de base de datos o no, y el momento en que se deben aplicar. i. 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 Almacenamiento de IOPS aprovisionadas (SSD). j. El servicio debe permitir aprovisionar almacenamiento adicional. k. El servicio debe permitir crear una o varias réplicas de un recurso de cómputo de base de datos de origen determinado y abastecer el alto volumen de tráfico de lectura de la aplicación desde distintas copias de sus datos, lo cual aumenta el rendimiento de lectura total. l. El servicio debe permitir hacer copias de seguridad automatizadas. m. El servicio debe permitir realizar una copia de seguridad de los registros de base de datos y de transacciones y los debe poder almacenar durante un periodo de retención que puede especificar el usuario. n. El servicio debe permitir especificar el periodo de retención de copia de seguridad automática hasta un máximo de 30 días. o. 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. p. El servicio debe permitir cifrar las bases de datos mediante las claves. q. El servicio debe permitir que los datos almacenados en reposo en el almacenamiento subyacente estén cifrados, al igual que las copias de seguridad automatizadas, las réplicas de lectura y las instantáneas. r. El servicio debe soportar la capacidad de aislar la base de datos en la propia red virtual y conectarse a su infraestructura de TI local		

mediante las VPN con IPsec cifradas estándar del sector. s. El servicio debe ofrecer la posibilidad de controlar las acciones que realizan los usuarios y grupos. t. El servicio debe permitir controlar las acciones que pueden realizar los usuarios y grupos en grupos de recursos que tengan la misma etiqueta y valor asociado u. El servicio debe soportar herramientas de monitoreo que permitan monitorear métricas operativas clave, incluidos el uso de la capacidad de cómputo, memoria y almacenamiento, la actividad de E/S y las conexiones de instancias de bases de datos. v. El servicio debe soportar la capacidad de notificar eventos de la base de datos por email o SMS, los cuales deben ser enviados a un correo institucional. w. El servicio debe soportar el registro y auditoría de los cambios en la configuración de la instancia de base de datos, incluidos grupos de parámetros, grupos de subred, instantáneas, grupos de seguridad y suscripciones a eventos. x. El servicio debe soportar escalamiento horizontal. ● **Servicio de almacenamiento de Objetos** a. El servicio debe brindar acceso a una consola centralizada de copias de seguridad. b. Debe ser un almacenamiento basado en objetos de tipo S3 o S3 Compatible o Blob storage. c. Debe contar con 3 tipos de almacenamiento como mínimo: de uso frecuente o standard, de uso poco frecuente y tipo archive ó glacier. d. Debe tener una durabilidad de hasta 99,999999999% (11 9s) de los objetos en caso se usen varias zonas de disponibilidad e. El servicio debe contar con controles de seguridad que garantizan que las carpetas y objetos no tengan acceso público f. El servicio debe permitir copiar objetos entre carpetas, reemplazar conjuntos de etiquetas de objetos, modificar los controles de acceso y restaurar objetos archivados desde otros servicios de almacenamiento. g. El servicio debe contar con control de versiones que permitan preservar, recuperar y restaurar fácilmente todas las versiones de un objeto almacenado, lo que debe permitir recuperarse		

fácilmente de acciones de usuarios involuntarias y de errores de aplicaciones. • **Servicios de Balanceo de Carga** a. Debe permitir el balanceo de carga para distribuir el tráfico a distintas unidades de procesamiento. b. El servicio debe distribuir automáticamente el tráfico de aplicaciones entrantes a través de varios destinos, tales como instancias y direcciones IP. c. El servicio debe estar en capacidad de detectar destinos que funcionen incorrectamente, dejar de enviar tráfico a ellos y, a continuación, distribuir la carga entre los destinos restantes que no presenten problemas. d. Se podrán crear y administrar grupos de seguridad asociados con balanceadores de carga a fin de ofrecer opciones de seguridad y redes adicionales e. El servicio debe proporcionar la capacidad de administración integrada de certificados y descifrado SSL/TLS vigente y actualizado, lo que debe brindar la flexibilidad para administrar de manera centralizada los parámetros de SSL del balanceador de carga y eliminar el trabajo intensivo de la CPU de la aplicación. f. El servicio debe permitir equilibrar la carga en aplicaciones HTTP o HTTPS para características específicas de la capa 7. g. El servicio debe facilitar el monitoreo de rendimiento de las aplicaciones en tiempo real. h. El servicio debe proporcionar direccionamiento de solicitudes avanzado destinado a la entrega de arquitecturas de aplicaciones modernas, incluidos microservicios y aplicaciones basadas en contenedores i. El servicio debe asegurar que se utilicen en todo momento los protocolos y cifradores SSL/TLS más recientes. j. El servicio debe permitir distribuir el tráfico de entrada entre destinos en numerosas zonas de disponibilidad k. El servicio debe escalar automáticamente la capacidad de administración de solicitudes como respuesta al tráfico de aplicaciones entrante l. El servicio debe poder ser configurado para que se pueda obtener acceso a él desde Internet o crear un balanceador de carga sin direcciones IP		

públicas para que actúe como balanceador de carga interno (es decir, sin acceso a Internet) m. El servicio debe ser compatible con WebSockets n. El servicio debe direccionar el tráfico solamente a destinos que funcionan correctamente. o. El servicio debe facilitar el monitoreo de métricas tales como el recuento de solicitudes, el recuento de errores, los tipos de errores y la latencia de las solicitudes. ● **Servicio Web Application Firewall** a. Todas las aplicaciones descritas a nivel cloud y local deberán contar con este servicio. Actualmente solo cuentan con este servicio: ● datacocha.inaigem.gob.pe b. El servicio debe considerar en los puntos de entrada del tráfico web, de acuerdo a la arquitectura de aplicación, distribución y gestión del tráfico como Amazon CloudFront, Application Load Balancer o Amazon API Gateway. c. 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. d. El servicio debe permitir crear reglas que bloquean ataques comunes como la inyección SQL o el scripting entre sitios. e. El servicio debe permitir crear un conjunto centralizado de reglas que puede implementar en varios sitios web. f. El servicio debe poderse administrar por completo mediante API. g. 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 h. El servicio debe proporcionar métricas en tiempo real y registrar solicitudes sin procesar que incluyen detalles sobre direcciones IP, geolocalización, URI, agentes de usuario y árbitros. i. El servicio debe permitir agregar una lista de IP anónimas para las reglas administradas de la nube. j. El servicio debe permitir una rápida propagación de las reglas definidas.		

k. El servicio debe contar con protección de bot. l. El servicio debe integrarse con servicios de API gestionados. m. El servicio debe permitir descargar los logs para integrarlos a herramientas de terceros. n. El servicio debe soportar listas IP anónimas. o. El servicio debe soportar un centro de comandos de seguridad centralizado ● **Servicio de gestión de DNS** a. El servicio debe ser escalable y debe proveer alta disponibilidad. b. 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. c. 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 d. 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. e. 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. f. El servicio debe permitir dirigir automáticamente a los visitantes del sitio web a una ubicación alternativa para evitar interrupciones del servicio. g. El servicio debe permitir dirigir automáticamente a los visitantes del sitio web a una ubicación alternativa para evitar interrupciones del servicio. h. 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. i. El servicio debe contar con una sencilla interfaz de servicios web que permita ponerse en marcha en cuestión de minutos j. El servicio debe permitir transferir el dominio desde otro servicio DNS al servicio DNS en la nube		

Av, Centenario 2656 - Sector Palmira- Independencia Huaraz- Ancash - Perú
Av. Antonio Miró Quesada 457 - Oficina 401 Edificio Corporativo ABC LIma - LIma - Magdalena del Mar - Perú
Av. Industrial Nro. Mz. N Lt 1 Urb. Residencial Huancaro - Santiago - Cusco - Perú

k. El servicio debe ofrecer un conjunto sencillo de API que facilita la creación y la administración de registros DNS para los dominios l. El servicio debe incluir la funcionalidad de administración de nombres DNS para escalar hacia arriba o hacia abajo el microservicio. m. El servicio debe tener una disponibilidad del 99.9% como mínimo. ● **Servicios de Monitoreo y observabilidad** a. El servicio debe permitir a la entidad monitorear todos los recursos de base de datos de: SGD y Datacocha. b. 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. c. El servicio debe permitir visualizar y analizar el estado, el rendimiento y la disponibilidad en un solo lugar. d. El servicio debe permitir monitorear puntos de enlace de la aplicación. e. 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. f. El servicio debe permitir realizar análisis históricos para optimizar costos y obtener información en tiempo real sobre los recursos. g. El servicio debe permitir recopilar hasta 50 métricas predeterminadas de servicios de la nube. h. El servicio debe permitir crear gráficos reutilizables y ver los recursos de la nube en una vista unificada. i. El servicio debe permitir monitorear contenedores j. El servicio debe contar con granularidad configurable de monitoreo/alerta. k. 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. l. La funcionalidad de alarmas debe permitir definir un umbral de métricas y activar una acción.		

m. El servicio debe permitir monitorear el rendimiento operativo, resolver errores y detectar tendencias. n. El servicio debe permitir controlar qué usuarios y recursos tienen permiso para obtener acceso a sus datos y de qué manera lo hacen. o. El servicio debe permitir cifrar los datos en tránsito y en reposo. ● **Servicio SMTP** a. El servicio debe ser plenamente compatible con el protocolo SMTP estándar para permitir la integración con aplicaciones existentes. b. Debe ser capaz de manejar grandes volúmenes de correo electrónico, escalando automáticamente para adaptarse a las necesidades de tráfico de correo. c. Debe ofrecer robustas medidas de seguridad, incluyendo soporte para autenticación SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) y DMARC (Domain-based Message Authentication, Reporting and Conformance). d. El servicio debe ofrecer capacidades de monitoreo y generación de reportes detallados sobre las métricas de envío, como tasas de entrega, rebotes y quejas. e. Debe proporcionar APIs para permitir la automatización de tareas y la integración con otras aplicaciones y sistemas. f. Debe soportar el cifrado de los mensajes de correo electrónico durante el tránsito. ● **Servicio de entrega de contenido (CDN)** a. El servicio debe ofrecer una red global de puntos de presencia (PoPs) para asegurar la entrega rápida y eficiente de contenido a usuarios de todo el mundo. b. Debe garantizar un alto rendimiento y baja latencia en la entrega de contenido, optimizando la experiencia del usuario final. c. El servicio debe ofrecer capacidades avanzadas de caching para reducir la carga en los servidores de origen y mejorar los tiempos de respuesta. d. Debe proporcionar robustas medidas de seguridad, incluyendo la protección contra ataques de denegación de servicio distribuido		

(DDoS) y la integración con un Web Application Firewall. e. Capacidad para personalizar las reglas de caché y distribución de contenido para satisfacer necesidades específicas de aplicaciones. f. Ofrecer herramientas de análisis e informes detallados para monitorear y entender el uso del servicio, patrones de tráfico y rendimiento. g. El servicio debe ser compatible con los protocolos HTTP y HTTPS, permitiendo una transición segura y flexible entre ambos. ● **Servicio de transferencia de datos en la nube** a. El servicio debe permitir la transferencia de datos hacia y desde la infraestructura de proveedor cloud de manera eficiente y segura. b. Debe proporcionar opciones para la transferencia de datos a través de Internet y conexiones directas dedicadas. c. El servicio debe admitir la transferencia de datos en diferentes formatos, incluidos archivos, bases de datos y transmisiones en tiempo real. d. Debe ofrecer opciones de compresión y cifrado para garantizar la seguridad y la eficiencia de la transferencia de datos. e. El servicio debe ser compatible con la migración de datos hacia y desde otros proveedores de servicios en la nube y entornos locales. f. Debe proporcionar herramientas y recursos para supervisar y gestionar la transferencia de datos, incluida la optimización de la velocidad y el rendimiento. g. El servicio debe ser compatible con las políticas de seguridad de la organización, incluida la gestión de acceso y permisos. h. Debe ser facturado según el volumen de datos transferidos y la velocidad de transferencia de datos. Para la presentación de su oferta, el postor deberá presentar los costos totales, asumiendo el supuesto de que se usarán todos los servicios solicitados en los términos de referencia al 100%; para lo cual los postores deberán considerar de acuerdo al cuadro del ítem 6.2. En caso de que algún servicio/ componente de la infraestructura en nube deje de ser utilizado, estos créditos deben suplirse con otro servicio/ componente.		

6.2. Requisitos de capacidad

El Servicio de Infraestructura (IaaS) y alojamiento en la nube de INAIGEM incluye las siguientes características en los servicios a contratar:

Item	Componentes del Servicio			Unidad de medida	Cantidad Mensual referencial
1	Servicio de Instancias de cómputo	Sistema operativo	Linux	Cantidad	1
		vCPU	2		
		Memoria RAM	8 GB		
		Disco SSD	800 GB		
2	Servicio de Instancias de cómputo	Sistema operativo	Linux	Cantidad	4
		vCPU	2		
		Memoria RAM	4 GB		
		Disco SSD	30 GB		
3	Servicio de Instancias de cómputo	Sistema operativo	Windows server 2025	Cantidad	1
		vCPU	2		
		Memoria RAM	2 GB		
		Disco SSD	30 GB		
4	Servicio de Instancias de cómputo (DIGC)	Sistema operativo	Linux	Cantidad	1
		vCPU	2		
		Memoria RAM	2 GB		
		Disco SSD	20 GB		
5	Servicio de Instancias de cómputo (DIGC)	Sistema operativo	Linux	Cantidad	3
		vCPU	2		
		Memoria RAM	4 GB		
		Disco SSD	30 GB		
6	Servicio de Instancias de cómputo (DIGC)	Sistema operativo	Linux	Cantidad	2
		vCPU	2		
		Memoria RAM	8 GB		
		Disco SSD	50 GB		
7	Servicio de base de datos compatible con PostgreSQL (HA)	vCPU	2	Cantidad	1
		RAM	8 GB		
		SSD	100 GB		
		Zonas de disponibilidad	2		
8	Servicio de base de datos compatible con MYSQL	vCPU	2	Cantidad	1
		RAM	4 GB		
		SSD	100 GB		
		Zonas de disponibilidad	2		

9	Servicio de almacenamiento de objetos	Almacenamiento estándar de objetos (TB)	2 TB	Cantidad	1
		Solicitudes a la API de objetos	8 M		
10	Balanceador de carga a nivel de aplicación	Número de balanceadores de carga de aplicaciones	1	Cantidad	1
		GB procesados	500 GB		
11	Servicio de WAF	Número de solicitudes (HTTPS)	15M	Cantidad	1
		Reglas	4		
12	Servicio de gestión DNS	Hosted zones	4	Cantidad	1
13	Servicio de monitoreo y observabilidad	Paneles	1	Cantidad	1
		Datos de registros ingeridos (GB)	20 GB		
		Solicitudes a API de métricas	50		
		Alarmas	10		
14	Servicio SMTP	Cantidad de mensajes de correo enviados	3000	Cantidad	1
15	Servicio de CDN	Número de solicitudes (HTTPS)	10M	Cantidad	1
		Transferencia de datos a Internet (GB)	1000 GB	Cantidad	1
16	Servicio de transferencia de datos	Transferencia de datos salientes (GB)	600 GB	Cantidad	1
17	IPv4	Número de IP públicas	13	Cantidad	1
18	Servicio de Instancias de cómputo	Sistema operativo	Linux	Cantidad	1
		vCPU	2		
		Memoria RAM	8 GB		
		Disco SSD	800 GB		
		Uso mensual estimado	2 horas		
19	Servicio de base de datos compatible con PostgreSQL (HA)	vCPU	2	Cantidad	1
		RAM	8 GB		
		SSD	100 GB		
		Zonas de disponibilidad	2		
		Uso mensual estimado	2 horas		

Leyenda Nomenclaturas:
M = Millones
MB = Megabytes
GB = Gigabytes
TB = Terabytes
HA = High Availability
MS = Milisegundos

6.3. Implementación del servicio

El servicio contempla una etapa de implementación, donde el proveedor deberá desplegar los servicios solicitados en el numeral 6 en un plazo de no mayor a 30 días calendario contados a partir del día siguiente de la firma de contrato.

Responsabilidad del postor:

- Elaboración de un (01) plan de trabajo para la implementación del proyecto.
- Implementar la arquitectura y diseño de la solución con Infraestructura como Código (IaC) de los diversos componentes mencionados en el numeral 6 en ambiente PROD.
- Implementación y diseño del flujo de despliegue y entrega continua para los componentes de backend, frontend (CI/CD) en ambiente PROD.
- Las pruebas de estrés deberán permitir una observabilidad de la aplicación, y base de datos, para ello el proveedor deberá orquestar herramientas de Open Telemetry y/o similares para obtener métricas adecuadas.
- Realizar hasta una (01) prueba de ethical hacking y/o pentesting para las aplicaciones, con su informe técnico detallado los puntos de vulnerabilidad, clasificándolos y proponiendo soluciones de mitigación con los tiempos estimado de corrección.
- Informe técnico detallado con los puntos de mejora de la arquitectura a nivel de backend, APIs, frontend y base de datos.
- Configuración de Backups se deberá contar con la activación de Backups automáticos realizados de forma diaria, a una hora establecida:
  - ➔ Base de datos por un periodo de retención de 30 días y para los servidores de aplicaciones: 1 mensual por un periodo de retención de 3 meses para los ambientes de producción, con la posibilidad de modificar la hora en el momento oportuno que se requiera.
  - ➔ Para el proceso de Backups deberá incluir la base de datos, los repositorios de archivos (con una sincronización a cada hora) y los Sites publicados en las instancias virtuales del ambiente de Producción.
  - ➔ Los archivos backups deberán ser almacenados en repositorios de objetos destinados exclusivamente para almacenar este tipo de respaldos, los cuales podrán ser utilizados para restaurarse en el ambiente que se considere necesario. Los backups deben ser disponibilizados al INAIGEM para su acceso en cualquier momento , por lo que deben brindar una cuenta para acceder a los mismos.
- Brindar el soporte técnico 24/7 por el tiempo que dure el contrato.

6.3.1 Servicio de soporte

El Contratista proveerá un servicio de Soporte bajo las siguientes etapas.

- En caso se presentar una falla en el servicio, INAIGEM podrá comunicarse con el PROVEEDOR a través de los canales de atención formales y establecidos, todas las

incidencias y/o requerimientos deberán ser registrados en una herramienta de gestión de tickets.

- El PROVEEDOR deberá ofrecer un servicio de soporte que, como mínimo, sea equivalente a los niveles de soporte 'Enterprise' comúnmente ofrecidos en la industria de servicios de nube. Este servicio de soporte deberá incluir, entre otros, monitoreo de toda la infraestructura contratada, respuesta rápida a incidentes críticos, acceso a expertos técnicos y revisión periódica de la arquitectura y configuración de la infraestructura por la marca de la nube a ofertar.
- El PROVEEDOR debe tener la capacidad suficiente para la atención y resolución de todos los problemas que se presenten con la solución propuesta, los únicos casos que podrá reportar con el fabricante son los ocasionados por un mal funcionamiento del producto. Todos los casos reportados deberán ser escalados para que el servicio sea repuesto lo más pronto posible y en dicho caso PROVEEDOR realizará el seguimiento del caso e informará a INAIGEM enviando la siguiente información: Número de caso abierto, estado del caso reportado.
- El PROVEEDOR deberá contar con centro de atención de llamadas de reparación o asistencia técnica instalado de tal manera que le asegure a INAIGEM que se encuentra en condiciones de cumplir con lo estipulado.
- Este servicio deberá ser atendido a través de los siguientes Canales de Atención:
  - ➔ Telefónico, a través de un número de contacto disponible en modalidad 24x7. Este podrá ser número fijo o móvil y donde se podrá reportar y atender cualquier tipo de solicitud.
  - ➔ Correo electrónico, a través de una dirección de correo asignada para la atención de solicitudes (incidentes, requerimientos o consultas).
  - ➔ También podrá estar disponible atención vía web o vía chat. El proveedor deberá oficializar estos canales de atención al inicio del servicio.

6.3.1.1 Atención de requerimientos

De solicitar una petición que implique gestión de cambios. En general se considera que existen labores de “gestión de cambios” en aquellas solicitudes que tendrán las siguientes características:

- El trabajo solicitado debe ser ejecutado por el personal con perfil de especialista cloud.
- La duración de estas actividades no está acotada completamente, ya que dependen de la complejidad de la petición que INAIGEM demande.
- Como parte del servicio el proveedor debe atender los requerimientos como la implementación de mejoras en las aplicaciones, actualización de servidores y sistemas operativos, implementación de mejoras en la arquitectura, y mejoras a nivel de base de datos, que el área usuaria solicite por los canales indicados. El proveedor deberá disponer de una bolsa de 100 horas para la atención de estas solicitudes durante el periodo de servicio. El uso de estas horas deberá ser documentado y reportado en los entregables mensuales, especificando el detalle de las actividades realizadas. El proveedor deberá garantizar que, si no ha cubierto al menos el 75 % del total de horas contratadas hasta el noveno mes del contrato, deberá compensar las horas no utilizadas a la entidad, entregando un equivalente en créditos.

6.3.1.2. 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 recepcionado. Luego el personal especializado se comunicará con la entidad para informar que el requerimiento ha sido recepcionado 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: 8:00 am a 6:00 pm (L-V)

6.3.1.3 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 Nivel 1 (Graves): Fallos que involucran una indisponibilidad del servicio de infraestructura cloud.
- ➔ Severidad 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%.
- ➔ Severidad Nivel 3 (Leves): Fallos que involucran a funcionalidades secundarias del servicio y que no afectan su normal operatividad.

Estos niveles de severidad servirán a los grupos de operación para priorizar las incidencias y atenderlas en base a los siguientes tiempos de respuesta:

- Severidad Nivel 1: 30 min. en 7 x 24
- Severidad Nivel 2: 1 hora en 7 x 24
- Severidad Nivel 3: 2 horas en 8 x 5 y 4 horas 7 x 24

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 (*)

6.3.1.4 Resolución 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.

Urgencia del incidente	Tiempo solución máximo (**) no presencial
Alta	8 horas
Media	12 horas
Baja	24 horas

(**) El inicio del tiempo de solución se contabiliza a partir del tiempo de respuesta máximo correspondiente. Cubre incidentes de configuración en general no atribuibles al fabricante.

- **Alta:** Son incidentes que necesitan un tratamiento especial por lo que su impacto representa para la organización; su atención inmediata afecta o podría afectar significativamente la operación de algún componente de la infraestructura tecnológica.
- **Media:** Son incidentes con un tiempo de atención intermedio; su inatención afecta o podría afectar moderadamente a la operación de algún componente de la infraestructura tecnológica.
- **Baja:** Son incidentes con un tiempo de atención menor; su inatención afecta o podría afectar levemente a la operación de algún componente de la infraestructura tecnológica.

La clasificación de la urgencia la realizará el personal de la entidad en el registro del incidente de acuerdo al detalle del numeral 6.3.2. El personal verificará que se haya dado la solución al incidente antes de aceptar el fin del tiempo de solución.

6.3.2 Niveles de servicio y criticidad

Se deberán manejar los siguientes niveles de servicio:

Nivel	Detalle
ALTO	– Falla Conectividad de Aplicaciones. – Accesos servidores virtuales Truncados. – Aplicaciones fuera de servicio – Tiempo de Atención de requerimientos: 15 min. de respuesta de solicitud. – Tiempo de Solución de incidencias: Según nivel de criticidad puede variar entre 30 min. a 2 horas.
MEDIO	– Habilitación de Permisos. – Problemas en Tiempos de Respuesta. – Latencia alta. – Revisión de conectividad. – Tiempo de Atención de requerimientos: 30 min. de respuesta de solicitud. – Tiempo de Solución de Incidencias: según nivel de criticidad puede variar entre 1 hora. a 3 horas.
BAJO	– Activación de nuevos servicios o recursos. – Configuraciones en general. – Tiempo de atención de requerimientos: 60 min. de respuesta de solicitud. – Tiempo de Solución de Incidencias: según nivel de criticidad puede variar entre 2 horas a 6 horas.

Para cumplir con los niveles de servicio requeridos, el proveedor deberá proporcionar al menos lo siguiente:

- Un número telefónico principal y uno alterno (fijo o celular).
- Un correo electrónico para contactar en caso sea necesario para enviar requerimientos o coordinar atención de incidencias.
- Nombre del contacto principal y alterno.

El proveedor debe considerar:

- El Proveedor debe asignar especialistas en la infraestructura de nube implementada para resolver los incidentes reportados de manera oportuna y en cumplimiento de los niveles de servicio requeridos establecidos.
- El Proveedor debe contar con el planeamiento de contingencias y un plan de respaldo en caso de caída general de los servicios globales, esto mediante sus propios servicios hasta restablecer el nivel de servicio estipulado en los términos de referencia.
- El Proveedor deberá solucionar los incidentes que afectan el normal desempeño de la infraestructura y plataforma informática de nube implementada y hacer el seguimiento y escalamiento necesario para superar el incidente.

6.3.3 Requerimientos de seguridad

6.3.3.1 Seguridad de acceso

Se debe contar con mecanismos de seguridad para el acceso, además del acceso al portal de nube, a través de perfiles administrados. Existirá un permiso de tipo Administrator Access que deberá asignarse a la cuenta del personal de Infraestructura designado por el INAIGEM que representará al sysadmin (usuario con todos los permisos). También podrán habilitarse otros permisos de menor nivel para actividades específicas o de solo lectura sobre los otros componentes de la arquitectura.

Las prácticas de gestión de seguridad de información ofrecida por el proveedor deberán mitigar riesgos de ataques de Ip spoofing, escaneos de puertos, ataques de fuerza bruta y protección ante ataques de denegación de servicios, entre otros

El proveedor debe suministrar un sistema de seguridad lógica a través de firewalls de software robustos integrados y demás dispositivos, software o servicios en la nube que garanticen el flujo normal de la información, previniendo la interrupción o saturación del servicio.

6.3.3.2 Encriptación de datos

El proveedor deberá facilitar y realizar la implementación de los certificados en los respectivos servidores contratados. (instalación y configuración).

Así mismo el proveedor deberá ofrecer certificados SSL por parte del proveedor de la marca que permitan implementarse en los recursos propios de la marca de la nube a ofrecer.

6.3.3.3 Pruebas de vulnerabilidad

El INAIGEM deberá tener la potestad de realizar las pruebas de seguridad externas de vulnerabilidades y de intrusión y las pruebas de seguridad internas de la aplicación a través de un servicio de Ethical Hacking contratado por la entidad. Las credenciales de los accesos a las pruebas de vulnerabilidad serán solicitadas al correo de contacto del proveedor y deben ser entregadas con los permisos solicitados en un maximo de 24 hrs

En caso que se identifiquen vulnerabilidades como resultado de las pruebas de seguridad indicadas (en infraestructura), el proveedor deberá subsanarlos en un plazo máximo de 30 días calendario desde la identificación de las mismas.

6.3.3.4 Backups y restores

Luego de finalizado el servicio, el contratista debe realizar la descarga de toda la información de las aplicaciones incluidos los backups a los servidores on-premise o transferir la propiedad INAIGEM al proveedor ganador, esta actividad debe ser realizada como máximo en quince (15) días calendario y facilitar el acceso a las personas autorizadas de INAIGEM para acceder a los backups.

6.3.3.5 Recuperación de desastres

El proveedor deberá organizar y ejecutar una prueba de recuperación de desastres del aplicativo SGD una (01) vez al año. Esta prueba deberá basarse en la restauración del sistema a partir de los backups generados diariamente y deberá garantizar la recuperación tanto del servidor de aplicación como del servidor de base de datos, según lo especificado en los ítems 18 y 19 del cuadro de componentes indicados en el numeral 6.2.

Para ello:

- La entidad notificará al contratista sobre el inicio de la prueba con al menos 3 días de anticipación.
- El contratista será responsable de ejecutar la recuperación del aplicativo y garantizar su operatividad.
- El entorno restaurado deberá estar completamente funcional por un período máximo de 24 horas antes de su eliminación.
- La prueba debe incluir la validación de la integridad y consistencia de los datos recuperados, así como la verificación del correcto funcionamiento de los servicios y componentes del sistema.

El proveedor de servicios de la nube deberá emitir un informe detallado mediante correo electrónico dirigido a la Oficina de Tecnologías de la Información con copia al correo admin@inaigem.gob.pe, el cual debe incluir:

1. Tiempo total de recuperación (RTO - Recovery Time Objective) obtenido durante la prueba.
2. Punto de recuperación alcanzado (RPO - Recovery Point Objective), indicando la antigüedad de los datos restaurados.
3. Incidencias o desviaciones detectadas en el proceso de recuperación.
4. Recomendaciones de mejora para optimizar tiempos de respuesta y reducir impactos en caso de una contingencia real.
5. Registro de evidencias, incluyendo capturas de pantalla, logs de restauración y cualquier otro material que valide la correcta ejecución de la prueba.

6.3.3.6 Reportes

El Proveedor deberá presentar máximo hasta en un plazo de diez (10) días calendarios posteriores al término de cada servicio mensual, un INFORME MENSUAL DETALLADO DEL SERVICIO vía correo electrónico al Jefe de la Oficina de Tecnologías de la Información con copia al correo admin@inaigem.gob.pe, , el cual debe contener, como mínimo, lo siguiente:

- El proveedor deberá presentar un reporte de rendimiento de la infraestructura de los últimos 30 días, donde considere métricas como CPU, RAM, DISCO, RED, de los diversos servicios desplegados.
- El proveedor deberá presentar un registro con las incidencias reportadas por la entidad durante el mes.
- Reporte de consumo de cada mes.
- Reporte de consumo de cada mes detallado por cada servicio según lo indicado en el numeral 6.2.

- Reporte de atención de requerimientos.
- Informe de recuperación de desastres (1 al año) de acuerdo al ítem 6.3.3.5 a cargo del arquitecto de nube.
- Recomendaciones y/o sugerencias.

6.3.4 Etapas del servicio

El servicio requerido en la nube, contará con las siguientes etapas:

6.3.4.1 Transición de entrada

A efectos de transferir el servicio en la nube vigente, a la nube del contratista, se deberán considerar las actividades de implementación y continuidad de los servicios del INAIGEM.

6.3.4.2 Ejecución del servicio

El servicio de hospedaje en la nube brindado por el contratista, se inicia al día siguiente notificada la orden de servicio o lo que indica el contrato por un plazo de 12 meses y/o hasta agotar el monto total de capacidades de cómputo contratado, y es contabilizado en tramos mensuales.

6.3.4.3 Transición de salida

Antes del término de los 12 meses y/o hasta agotar el monto total de capacidades de cómputo contratado del servicio de hospedaje en la nube, y a efectos de transferir éste hacia la infraestructura que se proporcione posteriormente, el contratista deberá elaborar un plan de transición de salida, el cual deberá ser entregado al INAIGEM al menos 15 días calendarios antes de su ejecución.

La transición de salida deberá iniciarse como mínimo, 15 días calendarios antes de culminar el último tramo del servicio (último mes).

El plan de salida consiste en elaborar una lista secuencial de actividades a ser ejecutadas para llevar la infraestructura de las aplicaciones del INAIGEM al nuevo servicio, y describir las características vigentes del servicio en el momento de la elaboración del referido plan.

El contratista deberá brindar las facilidades necesarias para la migración de los servicios según lo indicado en el numeral 6.2. a las instalaciones del nuevo IaaS, según el Plan de salida elaborado.

6.4. Documentos entregables (Físico y/o Digital).

- **Implementación:** Presentar máximo hasta en un plazo de treinta (30) días calendarios a partir del día siguiente notificada la orden de servicio o lo que indica el contrato, la documentación pertinente, la cual debe contener, como mínimo, lo siguiente:
  - ➔ Plan de trabajo para la implementación del proyecto.
  - ➔ Arquitectura y diseño de la solución implementada a detalle.
  - ➔ Diseño del flujo de despliegue y entrega continua.
  - ➔ Resultados de la prueba de estrés end-to-end (con gráficas).

- ➔ Informe técnico detallado con los puntos de mejora de la arquitectura a nivel de backend, APIs, frontend y base de datos.
- ➔ Informe técnico detallado con los puntos de vulnerabilidad identificados en las pruebas de ethical hacking y alternativas de solución.
- ➔ Carta de Garantía y soporte técnico 24/7 según lo indicado en ítem 6.3.1
- ➔ Manual de usuario para la administración y gestión de recursos en la nube debe incluir los datos de Personal de contacto de acuerdo al Ítem 6.3.1.
- ➔ Voucher del examen de certificación AWS Solutions Architect - Associate para cuatro (04) participantes.
- ➔ Acta de Conformidad de Implementación.
- ➔ Certificaciones de cumplimiento de los estándares detallados en el numeral 6.1.
- ➔ Carta y/o certificado de respaldo como partner avanzado oficial de la marca (fabricante) de la nube pública a ofertar.

6.5. Lugar y plazo de ejecución de la prestación

6.5.1. Lugar:

El servicio se ejecutará para la entidad INAIGEM, ubicada en el ubicada en Av. Centenario N° 2656, Sector Palmira - Independencia - Huaraz - Ancash

El servicio será activado e implementado de manera remota en coordinación con el representante de la Oficina de Tecnologías de la Información.

6.5.2. Plazo:

6.5.2.1. Inicio del servicio:

Los servicios materia de la presente contratación se prestarán en el plazo de 365 días calendario, contados a partir del día siguiente notificada la orden de servicio o lo que indica el contrato.

6.5.2.2. Implementación:

- La implementación del servicio será realizada en un plazo máximo de hasta treinta (30) días calendarios, contados a partir del día siguiente notificada la orden de servicio o lo que indica el contrato, para lo cual finalizado el plazo establecido la OTI y el proveedor suscribirán el Acta de Conformidad de Implementación (Anexo A).

7. Requisitos y recursos del proveedor

Deberán ser presentados durante la etapa de presentación de las ofertas.

7.1 Requisitos del proveedor

- Tener experiencia en el servicio de implementación en la nube.
- Registro Único de Contribuyentes (RUC) habilitado.
- Código de Cuenta interbancario registrado y vinculado a su N° de RUC.
- Registro Nacional de Proveedores (RNP) vigente.
- Contar una carta de respaldo de la marca de nube a ofertar, en la cual acredite la experiencia del postor.

Acreditación

El postor deberá contar con carta y/o certificado de respaldo como partner avanzado oficial de la marca (fabricante) de la nube pública a ofertar.

7.2 Perfil del proveedor

Empresa especializada en brindar servicios de infraestructura en nube, servicios cloud computing y/o servicios similares en el Sector Público o Privado.

7.3 Personal requerido

1 Gerente de proyecto

Formación Académica: Profesional titulado en ingeniería en software o ingeniería en sistemas o ingeniería en sistemas de información o ingeniería informática o ingeniería electrónica o licenciado en computación o afines, con certificación oficial de gestión de proyectos PMP o Scrum Master vigente.

1 Arquitecto de nube

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, con certificación oficial como AWS Certified Solutions Architect - Professional vigente.

1 Especialista de nube

Formación Académica: Profesional titulado o bachiller en las siguientes carreras: Ingeniería de Software o Ingeniería de Sistemas o Ingeniería Electrónica o Ingeniería de Redes y Comunicaciones o afines, con certificación oficial como AWS Certified Solutions Architect - Professional vigente.

Acreditación:

El Título Bachiller, será verificado por el comité de selección 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.pej/ o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente línk: http://www.titulosinstitutos.pe/, según corresponda.

8. Requisitos de Calificación

8.1 Experiencia del postor en la especialidad

- El postor debe acreditar un monto facturado de S/ 100,000.00 (Cien mil con 00/100 soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda (versión inicial).
- En el caso de postores que declaren en el anexo “Declaración Jurada del Postor” tener la condición de micro y pequeña empresa se acredita una experiencia de S/

10,000.00 (Diez mil con 00/100 soles), por los servicios iguales y similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda (versión inicial).

➔ Se consideran servicios similares: experiencia en la implementación de proyectos de nubes privadas, nubes mixtas y/o 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 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.

8.2 Experiencia del personal clave

Gerente de proyecto

➔ **Experiencia:** Mínima de tres (03) años en gestión de proyectos informáticos o de tecnología de información.

➔ **Actividades a desarrollar:**

- Estará a cargo de la dirección general del proyecto, será el encargado de efectuar las coordinaciones directas con la Oficina de Tecnología de la Información, durante la etapa de la implementación.
- Informará sobre el avance de la implementación.
- Elaborará las actas.
- 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.

Arquitecto de nube

➔ **Experiencia:** mínima de tres (03) años en desarrollo y/o arquitectura y/o implementación y/o configuración y/o instalación de soluciones en nube o soluciones de cloud o soluciones de cloud computing o infraestructura en nube.

➔ **Actividades a desarrollar:**

- Realizará las coordinaciones con el personal de la Oficina de Tecnología de la Información.
- Responsable de las arquitecturas de la solución.

- Desarrollará toda la infraestructura como código (IaC) para la homologación de los ambientes en nube.
- 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 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.

Especialista de nube

➔ **Experiencia:** Deberá acreditar experiencia mínima de 3 años en administrador y/o desarrollador y/o operador y/o configuración y/o instalación de desarrollo y/o infraestructura en nube o soluciones de cloud o soluciones de cloud computing o infraestructura en nube.

➔ **Actividades a desarrollar:**

- Responsable de la implementación de niveles de infraestructura de la plataforma.
- Realizará las recomendaciones de buenas prácticas en nube mediante un informe mensual.
- Pruebas de ingeniería del caos en la solución implementada.
- Establecer sistemas de monitorización y alertas para las arquitecturas en la nube para detectar y responder rápidamente a cualquier problema o interrupción.
- Revisar y gestionar los costos asociados con las soluciones en la nube, recomendando optimizaciones cuando sea necesario.
- Elaboración de la documentación de la solución implementada.

Acreditación:

La experiencia del personal se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal clave propuesto.

9. Adelantos

El INAIGEM, **no otorga adelantos** o parte de pago por la adquisición del servicio.

10. Conformidad de la prestación del servicio

La conformidad del servicio la otorgará la Oficina de Tecnologías de la Información del INAIGEM, en un plazo no mayor a 10 días calendario posterior a la presentación de los entregables de implementación.

11. Forma de pago.

El pago se realizará en una (01) sola armada, posterior a la conformidad del entregable de implementación, de acuerdo al formato previsto para tal fin, sin embargo, ello no enerva el derecho a reclamar posteriormente por vicios ocultos.

12. Penalidades aplicables.

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

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

Donde F tiene los siguientes valores:

a) Para plazos menores o iguales a sesenta (60) días, para bienes y servicios en general: F = 0.40.

b) Para plazos mayores a sesenta (60) días, para bienes y servicios en general: F = 0.25.

13. Confidencialidad.

Al ser el INAIGEM, una entidad dedicada a la Investigación, el proveedor se obliga a guardar la confidencialidad y reserva absoluta en el manejo de información y documentación a la que se tenga acceso y que se encuentre relacionada con la prestación, quedando expresamente prohibido revelar dicha información a terceros.

14. Responsabilidad por vicios ocultos

El plazo máximo de responsabilidad del proveedor por la calidad ofrecida y por los vicios ocultos de los bienes entregados es de un (1) año contado a partir de la conformidad otorgada

15. Clausula Única: Anticorrupción:

Con la elaboración y notificación de la Orden de Compra se formaliza el vínculo contractual, para lo cual se incluirá el siguiente texto:

"Con la notificación de la presente, El Proveedor, declara y garantiza no haber, directa o indirectamente, haber negociado o efectuado, cualquier pago o, en general, cualquier beneficio o incentivo ilegal en relación al contrato.

EL Proveedor, se obliga a conducirse en todo momento, durante la ejecución del contrato, con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente.

EL Proveedor, se Compromete a: (i) comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y (ii) adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas.

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

16. Anexos

Con la elaboración y notificación de la Orden de Compra se formaliza el vínculo contractual, para lo cual se incluirá el siguiente texto:

- Anexo A: Acta de Conformidad de Implementación

ACUERDO 01

ACUERDO DE CONFIDENCIALIDAD Y SEGURIDAD DE INFORMACIÓN

1. CLÁUSULA DE CONFIDENCIALIDAD DE LA INFORMACIÓN

El CONTRATISTA y su personal se obligan a mantener y guardar estricta reserva y absoluta confidencialidad sobre todos los documentos e informaciones del INAIGEM a los que tenga acceso en ejecución del presente contrato. En tal sentido, el CONTRATISTA y su personal deberán abstenerse de divulgar tales documentos e informaciones, sea en forma directa o indirecta, a personas naturales o jurídicas, salvo autorización expresa y por escrito del INAIGEM. Asimismo, el CONTRATISTA y su personal convienen en que toda la información suministrada en virtud de este contrato es confidencial y de propiedad del INAIGEM, no pudiendo el CONTRATISTA y su personal usar dicha información para uso propio o para dar cumplimiento a otras obligaciones ajenas a las del presente contrato.

Los datos de carácter personal entregados por el INAIGEM a el CONTRATISTA y su personal, y los obtenidos por estos durante la ejecución de los servicios derivados de la adquisición; única y exclusivamente podrán ser aplicados o utilizados para el cumplimiento de los fines del contrato suscrito con el INAIGEM.

El CONTRATISTA se compromete a cumplir con lo indicado en la Ley N° 29733, Ley de protección de datos personales.

El CONTRATISTA deberá adoptar las medidas de índole técnica y organizativa necesarias para que sus trabajadores, directores, accionistas, proveedores y en general, cualquier persona que tenga relación con el CONTRATISTA no divulgue a ningún tercero los documentos e informaciones a los que tenga acceso, sin autorización expresa y por escrito del INAIGEM, garantizando la seguridad de los datos de carácter personal y evitar su alteración. Asimismo, El CONTRATISTA y su personal se hacen responsables por la divulgación que se pueda producir, y asumen el pago de la indemnización por daños y perjuicios que la autoridad competente determine.

El CONTRATISTA se compromete a devolver todo el material que le haya proporcionado el INAIGEM a la culminación o resolución del contrato, sin que sea necesario un requerimiento previo. Sin embargo, el CONTRATISTA se encuentra facultado a guardar copia de los documentos de la prestación del servicio brindado, siendo el INAIGEM la única que pueda acceder a dicha información. Dicha copia no puede ser dada a terceros, salvo autorización expresa y por escrito del INAIGEM.

La obligación de confidencialidad establecida en la presente cláusula seguirá vigente incluso luego de la culminación del presente contrato.

El incumplimiento de lo establecido en la presente cláusula, por parte del CONTRATISTA y su personal, constituye causal de resolución del presente contrato.

2. CLÁUSULA DE SEGURIDAD DE LA INFORMACIÓN

EL CONTRATISTA se compromete a respetar y aplicar de los servicios derivados de la adquisición, las políticas, procedimientos y controles de los sistemas de gestión, metodologías, estándares y otros establecidos por el INAIGEM y que declara conocer y aceptar.

Con la previa evaluación y conformidad respectiva, del INAIGEM autorizará todos los accesos a recursos o herramientas propias de la institución y que son requeridos por EL CONTRATISTA para la prestación de los servicios derivados de la adquisición . Una vez finalizado el contrato, todos los accesos serán retirados.

EL CONTRATISTA debe tomar medidas de protección de la información del INAIGEM que se encuentre almacenada en los equipos y/o dispositivos que requieran mantenimiento fuera de las instalaciones del INAIGEM, para ello debe cumplir con las políticas específicas de seguridad de la información establecidas para tal fin.

EL CONTRATISTA debe reportar incidentes, eventos u otro riesgo potencial de seguridad de la información para el INAIGEM a fin de realizar la investigación correspondiente.

EL CONTRATISTA se compromete, a brindar todas las facilidades necesarias para que el INAIGEM audite y/o monitoree los aspectos de seguridad de la información de los servicios derivados de la adquisición e información materia del contrato y los aspectos de almacenamiento de datos.

El CONTRATISTA exime de toda responsabilidad al INAIGEM, sus empleados y funcionarios, por cualquier litigio, acción legal o procedimiento administrativo, reclamación o demanda que pudiera derivarse de cualquier trasgresión o supuesta trasgresión de cualquier patente, uso de modelo, diseño registrado, marca registrada, derechos de autor o cualquier otro derecho de propiedad intelectual que estuviese registrado o de alguna otra forma existente a la fecha del contrato debido a la instalación del bien por parte del CONTRATISTA o el uso de los mismos por parte del INAIGEM.

El CONTRATISTA garantiza al INAIGEM que los servicios derivados de la adquisición, respetarán todos los derechos de propiedad intelectual referidos en el Decreto Legislativo N° 822 – Ley sobre el Derecho de Autor, normas modificatorias y complementarias; por lo que se compromete a garantizar que todo el software y las herramientas utilizadas no vulneran ninguna normativa, contrato, derecho, interés, patentes, legalidad o propiedad de terceros referidos en el decreto en mención.

_____

EL CONTRATISTA

www.gob.pe/inaigem

Av, Centenario 2656 - Sector Palmira- Independencia Huaraz- Ancash - Perú
Av. Antonio Miró Quesada 457 - Oficina 401 Edificio Corporativo ABC LIma - LIma - Magdalena del Mar - Perú
Av. Industrial Nro. Mz. N Lt 1 Urb. Residencial Huancaro - Santiago - Cusco - Perú

ACUERDO 02

ACUERDO DE CONFIDENCIALIDAD Y SEGURIDAD DE INFORMACIÓN PARA EL PERSONAL DESTACADO POR EL PROVEEDOR

Conste por el presente documento, un Acuerdo de Confidencialidad y Seguridad de Información que celebran de una parte el Instituto Nacional de Investigación de Glaciares y Ecosistemas de Montañas - INAIGEM, en adelante INAIGEM, con RUC Nº 20600404262, con domicilio legal en […….....] Provincia de […….....]. Departamento de Áncash - Perú, , representada por [……..…], identificado con DNI Nº […….], y de otra parte [.....], con DNI N° [……..], con domicilio en […….....] a quien en adelante se le denominará el PERSONAL DEL PROVEEDOR, en los términos y condiciones siguientes:

ANTECEDENTES

El PERSONAL DEL PROVEEDOR declara estar vinculado contractualmente con la empresa [……], que presta .[…….....], derivado del proceso […….....], según Contrato celebrado el […….....].

En atención a las declaraciones expuestas, acuerdan:

1. CONFIDENCIALIDAD

El PERSONAL DEL PROVEEDOR se obliga a mantener y guardar estricta reserva y absoluta confidencialidad sobre todos los documentos e informaciones del INAIGEM a los que tenga acceso en ejecución de los servicios derivados de la adquisición . En tal sentido, el PERSONAL DEL PROVEEDOR deberá abstenerse de divulgar tales documentos e informaciones, sea en forma directa o indirecta, a personas naturales o jurídicas, salvo autorización expresa y por escrito del INAIGEM. Asimismo, EL PERSONAL DEL PROVEEDOR conviene en que toda la información suministrada en virtud del contrato suscrito con el INAIGEM, es confidencial y de propiedad del INAIGEM, no pudiendo el PERSONAL DEL PROVEEDOR usar dicha información para uso propio o para dar cumplimiento a otras obligaciones ajenas al contrato.

Los datos de carácter personal entregados por el INAIGEM al PERSONAL DEL PROVEEDOR, y los obtenidos por estos durante la ejecución de los servicios derivados de la adquisición, única y exclusivamente podrán ser aplicados o utilizados para el cumplimiento de los fines del contrato suscrito con el INAIGEM.

El PERSONAL DEL PROVEEDOR se compromete a cumplir con lo indicado en la Ley N° 29733, Ley de protección de datos personales.

La obligación de confidencialidad establecida en el presente acuerdo seguirá vigente incluso luego de la culminación del contrato.

El incumplimiento de lo establecido en el presente acuerdo, por parte del PERSONAL DEL PROVEEDOR, constituye causal de resolución del contrato.

www.gob.pe/inaigem

Av, Centenario 2656 - Sector Palmira- Independencia Huaraz- Ancash - Perú
Av. Antonio Miró Quesada 457 - Oficina 401 Edificio Corporativo ABC LIma - LIma - Magdalena del Mar - Perú
Av. Industrial Nro. Mz. N Lt 1 Urb. Residencial Huancaro - Santiago - Cusco - Perú

2. SEGURIDAD DE INFORMACIÓN

El PERSONAL DEL PROVEEDOR se compromete a respetar y aplicar en los servicios derivados de la adquisición las políticas, procedimientos y controles de los sistemas de gestión, metodologías, estándares y otros establecidos por el INAIGEM y que declara conocer y aceptar.

Con la previa evaluación y conformidad respectiva, el INAIGEM autorizará todos los accesos a recursos o herramientas propias de la institución y que son requeridos por el PERSONAL DEL PROVEEDOR para la prestación del presente servicio derivados de la adquisición. Una vez finalizado el contrato, todos los accesos serán retirados.

El PERSONAL DEL PROVEEDOR debe tomar medidas de protección de la información del INAIGEM que se encuentre almacenada en los equipos y/o dispositivos que requieran mantenimiento fuera de las instalaciones del INAIGEM, para ello debe cumplir con las políticas específicas de seguridad de la información establecidas para tal fin.

El PERSONAL DEL PROVEEDOR debe reportar incidentes, eventos u otro riesgo potencial de seguridad de la información para el INAIGEM a fin de realizar la investigación correspondiente.

El PERSONAL DEL PROVEEDOR se compromete, a brindar todas las facilidades necesarias para que el INAIGEM audite y/o monitoree los aspectos de seguridad de la información de los servicios e información materia del contrato derivados de la adquisición y los aspectos de almacenamiento de datos.

El PERSONAL DEL PROVEEDOR exime de toda responsabilidad al INAIGEM, sus empleados y funcionarios, por cualquier litigio, acción legal o procedimiento administrativo, reclamación o demanda que pudiera derivarse de cualquier trasgresión o supuesta trasgresión de cualquier patente, uso de modelo, diseño registrado, marca registrada, derechos de autor o cualquier otro derecho de propiedad intelectual que estuviese registrado o de alguna otra forma existente a la fecha del contrato debido a la instalación del bien por parte del PERSONAL DEL PROVEEDOR o el uso de los mismos por parte del INAIGEM.

El PERSONAL DEL PROVEEDOR garantiza al INAIGEM que durante los servicios derivados de la adquisición brindará, respetará todos los derechos de propiedad intelectual referidos en el Decreto Legislativo N° 822 – Ley sobre el Derecho de Autor, normas modificatorias y complementarias; por lo que se compromete a garantizar que todo el software y las herramientas utilizadas no vulneran ninguna normativa, contrato, derecho, interés, patentes, legalidad o propiedad de terceros referidos en el decreto en mención.

Se firma el presente documento, en Lima a los [...] días del mes de [...] del [……...].

INAIGEM	PERSONAL DEL PROVEEDOR

www.gob.pe/inaigem

Av, Centenario 2656 - Sector Palmira- Independencia Huaraz- Ancash - Perú
Av. Antonio Miró Quesada 457 - Oficina 401 Edificio Corporativo ABC LIma - LIma - Magdalena del Mar - Perú
Av. Industrial Nro. Mz. N Lt 1 Urb. Residencial Huancaro - Santiago - Cusco - Perú

ANEXO A

ACTA DE CONFORMIDAD DE IMPLEMENTACIÓN

Se deja constancia que la empresa…… con Registro Único de Contribuyente (RUC) N° ……con domicilio en……que en su condición de Contratista ha cumplido con la implementación del SERVICIO DE INFRAESTRUCTURA EN NUBE PARA LOS SISTEMAS INFORMÁTICOS DE LA ENTIDAD, de acuerdo a lo requerido en los Términos de Referencia y a lo establecido en su propuesta técnica finalmente adjudicada.

Así también a la fecha, se deja constancia del buen funcionamiento de la indicada implementación cuenta con una garantía de los servicios y vicios ocultos que se pueda presentar después de suscrita la presente acta.

Firman dando fe de lo anterior, firman las partes.

Lugar y Fecha

……	……
SELLO Y FIRMA	SELLO Y FIRMA
Representante Legal Contratista	Oficina de Tecnología de la Información.