REQUERIMIENTO DE SERVICIOS – TÉRMINOS DE REFERENCIA

1. Datos Generales de la Contratación:

1.1. Denominación de la Contratación	SERVICIO DE INFRAESTRUCTURA EN NUBE PARA LA PLATAFORMA INFORMÁTICA
1.2. Área Usuaria (Unidad Orgánica)	Dirección de Información y Gestión del Conocimiento
1.3. Meta Presupuestaria	0006 - DIGC
1.4. Actividad del POI	AOI00163000175
1.5. Persona responsable del requerimiento su supervisión y seguimiento	SDIA - DIGC
1.6. Persona que otorgará la Conformidad	SDIA - DIGC

2. Finalidad Pública

Este servicio se enfoca en garantizar el funcionamiento óptimo de las plataformas de información de la institución, alojadas en servidores en la nube. Estas plataformas tienen la finalidad de almacenar y distribuir los resultados de investigaciones sobre glaciares y ecosistemas de montaña. El objetivo es asegurar la disponibilidad continua de estas plataformas, que son una fuente esencial de conocimiento técnico y científico para académicos, tomadores de decisiones y el público en general.

3. Antecedentes:

En el 2019, se implementó el repositorio institucional del INAIGEM, disponible en https://repositorio.inaigem.gob.pe. Esta plataforma sirve para almacenar y distribuir documentos técnicos importantes relacionados con glaciares y ecosistemas de montaña. Fue el primer servicio de información institucional implementado, funcionando íntegramente en la nube. Además, cumple con las disposiciones de la Ley Nº 30035, que regula el Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto."

En el 2021, se lanzó el sistema INAIGEM-CRIS, un servicio de información para mapear, registrar y publicar activos estratégicos generados por investigaciones científicas. Esta plataforma registra personas, equipos, laboratorios, publicaciones, patentes y otros activos de investigación. Su objetivo es fomentar redes colaborativas de investigación a nivel nacional e internacional. INAIGEM-CRIS fue la segunda plataforma de información desarrollada por la institución.

En el 2023, se inició con el proceso de implementación de la plataforma Datacocha, la cual tiene el objetivo de brindar el servicio de datos abiertos. Esta plataforma se alinea en la iniciativa de Gobernanza de Datos que promueve la PCM.

Actualmente, todas las plataformas operan en servidores informáticos en la nube y, en conjunto, facilitan la distribución y publicación de información sobre glaciares y ecosistemas de montaña. La adquisición de este servicio es de interés nacional, ya que mantiene activas y accesibles las valiosas fuentes de información y conocimiento producidas en el país.

Asimismo, este requerimiento se encuentra programado en el POI 2024, en la AOI00163000175 – Actualización e implementación de plataformas informáticas para la gestión de datos hidrometeorológicos, geoespaciales y documentos técnicos en glaciares y ecosistemas de montaña.

4. Objetivos de la Contratación

4.1. Objetivo General:

Contratar servicios de créditos de procesamiento en una infraestructura de nube pública para optimizar la operación y mantenimiento de los sistemas de información de la Dirección de Información y Gestión del Conocimiento. Esto facilitará la publicación eficiente de información técnica y científica, beneficiando así a la población en general.

4.2. Objetivo(s) Específico(s):

- ✓ Contratar créditos de procesamiento en una nube publica para asegurar el funcionamiento de los servicios de información del INAIGEM.
- ✓ Optimizar el flujo de información que se produce en el INAIGEM.
- ✓ Mantener operativos los sistemas de información existentes.

5. Características y condiciones del servicio a contratar

5.1. Descripción y cantidad del servicio a contratar

Descripción	Cantidad
SERVICIO DE INFRAESTRUCTURA EN NUBE PARA LA PLATAFORMA INFORMÁTICA **Capacidad de cómputo en la nube** Créditos de procesamiento para la creación, mantenimiento y operaciones de infraestructura de cómputo en la nube (5,580 créditos de procesamiento). **Duración de los créditos** Los créditos se agotan de acuerdo con el consumo de los sistemas de información. En caso no existe un consumo activo, los créditos se conservan indefinidamente. **Servicio Administrado de Nube (SAN)** Mediante esta funcionalidad es posible mantener el control y la supervisión de la infraestructura, los recursos y los servicios de computación en la nube en entornos de nube pública, privada o híbrida.	01

- La Infraestructura de Nube Pública descrita en los presentes términos de referencia deberá tener una disponibilidad mínima del 99.99%.
- 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 administrado por la Subdirección de Información y análisis y la Oficina de Tecnologías de la Información.
- 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:

Sede Central: Jr. Juan Bautista Mejía Nro. 887 Huaraz- Ancash – Perú Teléfono: (043) 221766
Oficina de Enlace Lima: Av. Del Pinar N° 134 – Oficina 804 – Santiago de Surco – Lima Teléfono: (01) 2883477

- El servicio de nube pública debe ser brindado por un proveedor de servicios de nube pública y debe estar debidamente acreditado en caso comercialice un servicio de terceros.
- 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 se proyecten 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).

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.
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.

Sede Central: Jr. Juan Bautista Mejía Nro. 887 Huaraz- Ancash – Perú Teléfono: (043) 221766
Oficina de Enlace Lima: Av. Del Pinar N° 134 – Oficina 804 – Santiago de Surco – Lima Teléfono: (01) 2883477

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 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 que protegen sus sitios web y aplicaciones en el proveedor de nube.

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.

Sede Central: Jr. Juan Bautista Mejía Nro. 887 Huaraz- Ancash – Perú Teléfono: (043) 221766
Oficina de Enlace Lima: Av. Del Pinar N° 134 – Oficina 804 – Santiago de Surco – Lima Teléfono: (01) 2883477

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.
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 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
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 base de datos en memoria

a. El servicio debe automatizar tareas como aprovisionamiento, configuración, parches y copias de seguridad.
b. El servicio debe ser totalmente compatible con Redis, permitiendo aprovechar todas sus funcionalidades y características.
c. Debe ofrecer cifrado en tránsito y en reposo, protegiendo los datos almacenados y en transmisión.
d. Soporte para herramientas de monitoreo avanzadas, permitiendo la visualización de métricas operativas clave.

Servicio de almacenamiento de Objetos

a. Debe ser un almacenamiento basado en objetos de tipo S3 o S3 Compatible o Blob storage.
b. Debe contar con 3 tipos de almacenamiento como mínimo: de uso frecuente o standard, de uso poco frecuente y tipo archive ó glacier.
c. Debe tener una durabilidad de hasta 99,999999999% (11 9s) de los objetos en caso se usen varias zonas de disponibilidad
d. El servicio debe contar con controles de seguridad que garantizan que las carpetas y objetos no tengan acceso público
e. 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.

Sede Central: Jr. Juan Bautista Mejía Nro. 887 Huaraz- Ancash – Perú Teléfono: (043) 221766
Oficina de Enlace Lima: Av. Del Pinar N° 134 – Oficina 804 – Santiago de Surco – Lima Teléfono: (01) 2883477

f. 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.

Servicio de almacenamiento de archivos

a. El servicio debe proporcionar almacenamiento elástico, escalando automáticamente para ajustarse al tamaño de los archivos almacenados sin necesidad de intervención manual.
b. Debe ser compatible con sistemas de archivos estándar y permitir el montaje en múltiples instancias de máquinas virtuales simultáneamente.
c. Debe ofrecer un rendimiento elevado y baja latencia, adecuado para aplicaciones y cargas de trabajo que requieran un acceso rápido y eficiente a archivos.
d. Debe garantizar una alta durabilidad y disponibilidad, almacenando los datos en múltiples zonas de disponibilidad.
e. Debe soportar protocolos de red estándar, como NFS, para facilitar la integración con sistemas existentes.

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, 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.

Sede Central: Jr. Juan Bautista Mejía Nro. 887 Huaraz- Ancash – Perú Teléfono: (043) 221766
Oficina de Enlace Lima: Av. Del Pinar N° 134 – Oficina 804 – Santiago de Surco – Lima Teléfono: (01) 2883477

Servicios VPN

a. El servicio debe permitir establecer conexiones seguras entre sus redes en las instalaciones de la entidad, las oficinas remotas, los dispositivos y la red global del proveedor de nube.
b. El servicio permite acceder ya sea con una configuración de IP Security (IPSec) de Site-to-Site VPN
c. El servicio soporta la conexión tanto de la Gateway privada virtual como de Transit Gateway.
d. El tráfico en el túnel entre los puntos de enlace debe poder encriptarse con AES128 o AES256 y utilizar protocolos Diffie-Hellman para intercambios claves
e. Para Site-to-Site VPN se debe autenticar mediante funciones SHA1 o SHA2
f. El servicio debe brindar opciones de túnel personalizables, incluidos dirección IP de túnel interna, clave compartida previamente y número de sistema autónomo para protocolo de Gateway fronteriza (BGP ASN)
g. El servicio opcionalmente debe contar con disponibilidad de rutas múltiples de igual costo (ECMP) con Site-to-Site VPN en la Transit Gateway para ayudar a incrementar la banda ancha de tráfico en varias rutas.
h. Site-to-Site VPN debe soportar aplicaciones transversales de NAT, de modo que pueda utilizar direcciones IP privadas, en redes privadas, detrás de enrutadores con una sola dirección IP pública con conexión a Internet.
i. Site-to-Site VPN debe permitir enviar métricas al servicio de monitoreo para ofrecer mayor visibilidad y supervisión.
j. Site-to-Site VPN debe soportar el uso de certificados privados
k. Site-to-Site VPN debe soportar encriptación IKE, IPsec y TLS
l. Conectividad Site to Site VPN: debe permitir conectarse localmente o desde la Entidad a la nube.

Servicio Web Application Firewall

a. 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.
b. El servicio debe permitir crear reglas que bloquean ataques comunes como la inyección SQL o el scripting entre sitios.
c. El servicio debe permitir crear un conjunto centralizado de reglas que puede implementar en varios sitios web.
d. El servicio debe poderse administrar por completo mediante API.
e. 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
f. 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.
g. El servicio debe permitir agregar una lista de IP anónimas para las reglas administradas de la nube.
h. El servicio debe permitir una rápida propagación de las reglas definidas.
i. El servicio debe contar con protección de bot.
j. El servicio debe integrarse con servicios de API gestionados.
k. El servicio debe permitir descargar los logs para integrarlos a herramientas de terceros.
l. El servicio debe soportar listas IP anónimas.
m. 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
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

a. El servicio debe permitir monitorear recursos de infraestructura locales, híbridos y de la nube.
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 de sus aplicaciones en un solo lugar.
d. 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)
e. El servicio debe permitir monitorear puntos de enlace de la aplicación
f. 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.
g. El servicio debe facilitar el diagnóstico, aislamiento y corrección de problemas
h. 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.
i. El servicio debe permitir recopilar hasta 50 métricas predeterminadas de servicios de la nube
j. El servicio debe permitir crear gráficos reutilizables y ver las aplicaciones y los recursos de la nube en una vista unificada
k. El servicio debe permitir monitorear contenedores
l. El servicio debe contar con granularidad configurable de monitoreo/alerta
m. 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

n. La funcionalidad de alarmas debe permitir definir un umbral de métricas y activar una acción.
o. El servicio debe permitir monitorear el rendimiento operativo, resolver errores y detectar tendencias
p. El servicio debe permitir controlar qué usuarios y recursos tienen permiso para obtener acceso a sus datos y de qué manera lo hacen
q. 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.

5.2. Actividades y procedimiento

5.2.1. Implementación del Servicio y Habilitación de Créditos

El proveedor debe desplegar y habilitar los créditos de procesamiento solicitados en el numeral 5 (literal 5.1).

5.2.2. Responsabilidad del postor:

Despliegue y habilitación de créditos de procesamiento de acuerdo con la cantidad requerida.

5.2.3. Análisis del funcionamiento de las instancias activas

- Implementación y diseño del flujo de despliegue y entrega continua para los componentes de backend, frontend (CI/CD) en dos (2) ambientes: QA / PROD.
- Realizar hasta dos (2) pruebas de estrés end-to-end en el ambiente QA para validar el rendimiento de la conexión VPN Site To Site, así como la comunicación con APIs externos.
- Las pruebas de estrés deberán permitir una observabilidad de la aplicación, APIs y base de datos, para ello el proveedor deberá orquestar herramientas de Open Telemetry y/o similares para obtener métricas adecuadas.
- Realizar hasta una (1) pruebas de ethical hacking y/o pentesting para la aplicación del MGD.
- 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 vulnerables o de mejora identificados en las pruebas de ethical hacking.
- Configuración de Backups automáticos realizados de forma diaria a una hora establecida de la base de datos por un periodo de retención de 30 días y para los servidores de aplicaciones 1 semanal por un periodo de retención de 2 meses.
- Brindar el soporte técnico 24/7 por el tiempo que dure el contrato.

5.3. Prestaciones accesorias a la prestación principal

5.3.1. 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 'Business' o 'Enterprise' comúnmente ofrecidos en la industria de servicios de nube. Este servicio de soporte deberá incluir, entre otros, 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.

5.3.2. 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.

5.3.3. 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 8:00 am a 6:00 pm (L-V)

5.3.4. 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 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 (*)

5.3.5. Capacitación

La capacitación solicitada será de manera presencial y/o remota, dentro del horario de oficina, para la cual el Proveedor coordinará previamente con INAIGEM, las fecha y hora para su realización.

Se deberá considerar la capacitación de hasta diez (10) colaboradores designados por la Dirección de Información y Gestión del Conocimiento en coordinación con la Oficina de Tecnología de la Información (OTI), la misma que constará de seis (12) horas como mínimo, en el que se abordarán los siguientes temas a continuación.

Syllabus capacitación:

- Servicio de Cómputo y Memoria
- Servicio de Almacenamiento
- Servicio de respaldo y recuperación
- Servicio de redes virtuales
- Servicio de balanceo de carga
- Servicio de base de datos relacionales y no relacionales
- Servicio de cómputo sin servidor
- Servicio de DNS
- Servicio de WAF

- ✓ La capacitación deberá ser coordinada con la Dirección de Información y Gestión del Conocimiento y y dentro de los veinte y cinco (25) días calendarios contados a partir del día siguiente de suscrita el Acta de Conformidad de Implementación **(Anexo-A).**

- ✓ Al final de la Capacitación, deberá entregarse una Constancia de participación a cada participante indicando el tiempo en horas y a la vez se deberá firmar un Acta de las Capacitación (**Ver Anexo C**), la cual será uno de los entregables (será requisito para la conformidad respectiva).

5.4. Lugar y plazo de ejecución de la prestación

5.4.1. Lugar: Este servicio no requiere la realización de actividades presenciales, excepto en situaciones donde la capacitación y el entrenamiento exijan el uso de las instalaciones físicas del INAIGEM, para este caso se debe considerar al siguiente dirección: Oficina central del INAIGEM, sito en la Av. Centenario 2656 - Sector Palmira, Independencia, Áncash - Huaraz - Independencia - Perú

5.4.2. Plazo: El servicio será ejecutado en un plazo de máximo de 30 (treinta) días calendario, contabilizados a partir del día siguiente de notificada la orden de servicio.

5.5. Resultados esperados

Los entregables serán presentados a través de mesa de partes virtual y/o física del INAIGEM, foliados y firmados en cada página, de acuerdo con el siguiente detalle:

- ✓ Reporte del despliegue y habilitación de créditos de procesamiento en la nube.
- ✓ Arquitectura de servicios disponibles de la SDIA-DIGC.
- ✓ 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.

6. Requisitos y recursos del proveedor

6.1. Requisitos del proveedor

- ✓ El proveedor, **deberá de dedicarse al rubro** de prestación de servicios iguales o similares al requerido.
- ✓ Registro Único de Contribuyentes (**RUC**) habilitado.
- ✓ Código de Cuenta Interbancario (**CCI**) registrado y vinculado a su número de RUC.
- ✓ Registro Nacional de Proveedores (**RNP**) vigente, en el capítulo de Servicios (Se excluye en el caso que el valor del servicio sea menor o igual a 1 UIT)

6.2. Perfil del proveedor:

- ✓ El postor debe acreditar un monto facturado de tres veces el valor estimado (en 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.
- ✓ 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 en s/ 30,000.00 (Treinta mil con 00/100 soles) por la venta de 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.

- ✓ 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.

- ✓ Se consideran servicios similares: experiencia en la venta y/o 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”.

6.3. Acreditación:

- ✓ La experiencia del postor en la especialidad se acreditará con copia simple de (1) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (i) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago, correspondientes a un máximo de veinte (20) contrataciones.

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

- ✓ Cuando estos contratos, órdenes de servicios o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta.

7. Consideraciones para la ejecución de la prestación

7.1. Obligaciones del Proveedor

El Proveedor es el responsable directo y absoluto de las actividades que realizará, ya sea directamente o a través de su personal, debiendo responder por el servicio brindado.

7.1.1. Medidas de seguridad

El Proveedor de la solución que debe considerar los Lineamientos para el Uso de Servicios de nube pública para entidades de la Administración Pública del Estado Peruano, para efectos de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad, por lo cual queda obligado a cumplir y demostrar que, como mínimo, cumple con todas las medidas de seguridad de la NTP ISO/IEC 27001:2014 Tecnología de la Información, pertinentes para el nivel de disponibilidad requerido. Esto incluye instalaciones y personal. En su defecto podrá presentar la certificación global para nubes públicas ISO/IEC 27001:2013 de la nube ofertada. El proveedor deberá ser un partner avanzado acreditado de la nube pública a ofertar. Las medidas de seguridad podrán ser reemplazadas por otras siempre y cuando se acredite con las certificaciones respectivas que protegen igual o mejor el riesgo sobre los activos y se satisfacen los principios básicos en materia de seguridad de la información antes señalada.

7.1.2. Confiabilidad

El Proveedor se obliga a mantener CONFIDENCIALIDAD sobre la documentación trabajada y su contenido es de plena responsabilidad, por lo que cualquier alteración de la misma será considerada como incumplimiento grave del contrato, motivo por el cual INAIGEM podrá resolver automáticamente el mismo, sin perjuicio de las sanciones y penalidades

El proveedor del servicio tiene y asume la obligación, tanto durante la vigencia del contrato, como después de su extinción, de guardar secreto y confidencialidad de cualquier información de INAIGEM a la que tenga acceso como consecuencia del desempeño de su servicio, y a considerar toda la información relativa a las cuentas de correo electrónico como información personal, especialmente la información relativa a personas recogida en ficheros de datos personales, cuentas de correo personales, datos técnicos y/u organizativos de INAIGEM.

Sede Central: Jr. Juan Bautista Mejía Nro. 887 Huaraz- Ancash – Perú Teléfono: (043) 221766
Oficina de Enlace Lima: Av. Del Pinar N° 134 – Oficina 804 – Santiago de Surco – Lima Teléfono: (01) 2883477

Por lo antes expuesto, el proveedor del servicio no podrá:

- Difundir, transmitir y/o revelar información a terceros.
- Usar la información recopilada para ofrecer promocionar o brindar información sobre productos o servicios.
- Arrendar ni vender a terceros ningún dato de identificación personal que les haya sido proporcionado por INAIGEM y/o como consecuencia del servicio brindado.
- Invitar al usuario a tomar parte en encuestas sobre productos, servicios, noticias y/o eventos.

8. Adelantos

El INAIGEM, **no otorga adelantos** o parte de pago por servicios que no sean efectivamente realizados.

9. **Conformidad de la prestación del servicio**

La conformidad de la prestación del servicio, la otorga el área usuaria, de acuerdo al formato previsto para tal fin, sin embargo, ello, no enerva el derecho a reclamar posteriormente por vicios ocultos.

10. Forma de pago.

El pago se realizará en una sola armada después de ejecutado el servicio y otorgada su conformidad, salvo que, por razones de mercado, el pago sea condición para la prestación del servicio.

11. 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 formula:

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

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.

12. 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.

13. Responsabilidad por vicios ocultos

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

14. Clausula Única: Anticorrupción:

Con la elaboración y notificación de la Orden de servicio 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."

www.inaigem.gob.pe
Sede Central: Jr. Juan Bautista Mejía Nro. 887 Huaraz- Ancash – Perú Teléfono: (043) 221766
Oficina de Enlace Lima: Av. Del Pinar N° 134 – Oficina 804 – Santiago de Surco – Lima Teléfono: (01) 2883477