ORGANISMO DE FORMALIZACIÓN DE LA PROPIEDAD INFORMAL - COFOPRI

TÉRMINOS DE REFERENCIA

Servicio de Plataforma en la Nube (PaaS) para Sistema Catastral

Proyecto de inversión denominado “Creación del servicio de catastro urbano en distritos priorizados de las provincias de Chiclayo y Lambayeque del Departamento de Lambayeque, la Provincia de lima del Departamento de Lima y la Provincia de Piura del Departamento de Piura”

Firmado digitalmente por BULEJE PUN Christian Enrico FAU 20306484479 soft
Motivo: Doy V° B°
Fecha: 09.11.2023 16:34:02 -05:00

Firmado digitalmente por NEIRA REYMER Jose Antonio FAU 20306484479 soft
Motivo: Doy V° B°
Fecha: 09.11.2023 16:46:13 -05:00

1. DENOMINACIÓN DE LA CONTRATACIÓN

Contratación del Servicio de Plataforma en la Nube (PaaS) para Sistema Catastral

2. OBJETO DE LA CONTRATACIÓN

El Organismo de Formalización de la Propiedad Informal COFOPRI a través de la Unidad Ejecutora 003, tiene por objeto la contratación del Servicio de Plataforma en la Nube (PaaS) para Sistema Catastral, con el fin de garantizar alta disponibilidad y escalabilidad en los servicios informáticos que soportan el Sistema Catastral.

REQUERIMIENTO

ÍTEM	DESCRIPCIÓN	CANTIDAD	U/M
01	Contratar una solución de Servicio de Plataforma en la Nube (PaaS) para Sistema Catastral	**01**	**Servicio**

3. FINALIDAD PÚBLICA

La Unidad Ejecutora 003 para el Proyecto de inversión denominado "Creación del servicio de catastro urbano en distritos priorizados de las provincias de Chiclayo y Lambayeque del Departamento de Lambayeque, la Provincia de lima del Departamento de Lima y la Provincia de Piura del Departamento de Piura" requiere contratar un servicio para provisión de administración e infraestructura en nube pública para los diversos servicios informáticos que permitirán la operación del Sistema Catastral.

4. ANTECEDENTES

Mediante el Decreto Supremo N° 050-2020-EF se aprobó la operación de Endeudamiento Externo a ser acordada con el Banco Internacional de Reconstrucción y Fomento (BIRF) destinada a financiar el PI "Creación del servicio de catastro urbano en distritos priorizados de las provincias de Lima, Chiclayo y Lambayeque del Departamento de Lambayeque; la Provincia de Lima del Departamento de Lima y la Provincia de Piura del Departamento de Piura", con código único de inversiones 2459010, con un costo total ascendente a US$ 50,000,000.00 (Cincuenta Millones y 00/100 Dólares Americanos) para cuyo financiamiento se ha suscrito con el BIRF el Convenio de Préstamo N° 9035-PE por la suma de US$ 50,000,000.00. Adicionalmente, el Estado Peruano financia con una contrapartida local de US$ 30,830,523 (Treinta millones ochocientos treinta mil quinientos veintitrés y 00/100 dólares americanos).

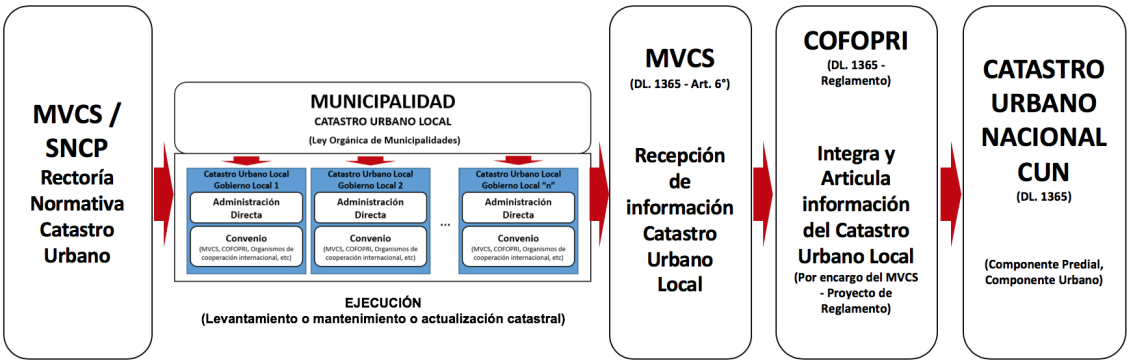
Con fecha 22 de mayo de 2020, se firma el Convenio de Préstamo N° 9035 entre el Banco Internacional de Reconstrucción y Fomento (BIRF) y el Gobierno de Perú, que financiará el PI "Creación del servicio de catastro urbano en distritos priorizados de las provincias de Chiclayo y Lambayeque del Departamento de Lambayeque; la Provincia de Lima del Departamento de Lima y la Provincia de Piura del Departamento de Piura".

El Ministerio de Vivienda, Construcción y Saneamiento (MVCS) es el órgano rector a nivel nacional de los catastros urbanos, encargado de implementar la estrategia de desarrollo de los catastros urbanos a nivel nacional. El Organismo de Formalización de la Propiedad Informal – COFOPRI ha

sido designado por el MVCS como la Unidad Ejecutora de Inversiones del presente proyecto de inversión pública.

Está definido que los actores involucrados en el proyecto son; los gobiernos locales, el Organismo de Formalización de la Propiedad Informal – COFOPRI y el Ministerio de Vivienda, Construcción y Saneamiento – MVCS

Ilustración: Articulación entre los actores involucrados del Proyecto



Fuente: D.L. 1365

- El Estudio de Pre inversión ha identificado debilidades, problemáticas y deficiencias que dificultan y limitan a las entidades públicas y privadas, poder tomar decisión en base a la información, estas deficiencias del catastro corresponden a:
- La debilidad de los sistemas de información de tierras impide que las distintas entidades que asignan derechos o establecen restricciones al uso de suelos puedan estar al tanto de lo que están haciendo las otras entidades, lo cual dificulta el diseño y armonización de políticas como la aplicación efectiva de las regulaciones.
- La carencia de una infraestructura de información de tierras (que incluye las normas, instituciones y sus roles, los sistemas de información y el acervo de datos) ha contribuido a que las principales ciudades crezcan descontroladamente sin que las instituciones oficiales hayan sido capaces de producir planes de desarrollo que se anticipen a la demanda.
- Un tercio de las municipalidades tienen asignados valores arancelarios por calles, aunque de manera incompleta o desactualizada. Sería razonable que el cálculo de los valores lo realicen las propias municipalidades que cuenten con las capacidades y que el rol del Ministerio de Vivienda, Construcción y Saneamiento sea el de un órgano rector.
- La existencia de una ficha catastral estándar para todas las municipalidades no reconoce la diversidad de las capacidades y necesidades de los gobiernos locales. Para la mayoría de las municipalidades, la exigencia de incluir los acabados en las fichas catastrales complejiza el proceso de cálculo del valor de las viviendas.
- La experiencia del Proyecto SIAF-GL (Sistema Integrado de Administración Financiera para los Gobiernos Locales) impulsado por el MEF ha demostrado que las municipalidades tienen la voluntad de ordenar su recaudación y que necesitan el acompañamiento y asistencia técnica. Uno de los problemas de la gestión del impuesto predial tiene que ver con la gran heterogeneidad de los gobiernos locales: mientras algunos distritos (especialmente en Lima y capitales de provincia) cuentan con catastros y capacidades técnicas que les permite recaudar eficientemente, hay otros que ni siquiera tienen un local donde operar.
- La falta de un sistema de catastro funcional dificulta completar el inventario de tierras del Estado. Se estima que el avance en la construcción del inventario no llegaría al 30% del total de propiedades del Estado. De un estimado de 8.5 millones de predios que tienen una partida registral

abierta en el Registro de Predios, más de la mitad carece de información catastral. Esto produce problemas frecuentes de superposición de derechos.

- Existe un alto nivel de desactualización del registro que amenaza la sostenibilidad de los programas de formalización. Las principales razones que explican que existen pocos incentivos para mantener los registros al día son los altos costos para formalizar las transacciones, y la falta de una "cultura registral".

El Proyecto de Inversión tiene como objetivo central "Mejorar la cobertura del Servicio de Catastro Urbano en distritos priorizados de Lima, Lambayeque, Chiclayo y Piura", y el fin de "Fortalecer los catastros urbanos en municipalidades priorizadas para mejorar las capacidades de los gobiernos locales para la generación de ingresos y la gestión urbana", como fin derivado del objetivo central del Proyecto.

Es preciso mencionar que "gestión urbana" comprende las actividades de planificación, control urbano y la gestión de riesgos de desastres naturales; y los fines directos del Proyecto son, (i) el incremento de la base tributaria del impuesto predial, y (ii) la adecuada información para la planificación y gestión del territorio.

Con el Proyecto se pretende satisfacer las necesidades a los tres niveles de gobierno y a la ciudadanía en general, a través de:

i) La mejora del marco institucional del catastro que incluya la revisión de las metodologías, procedimientos, estándares, etc.
ii) El fortalecimiento de las capacidades de las municipalidades en el procedimiento catastral, así como en el uso y aplicaciones en los procesos municipales.
iii) Generación de información y conocimiento del territorio que provea e integre información con las instituciones públicas y privadas, que facilite la fiscalización y la toma de decisiones.
iv) El desarrollo de mecanismos de simplificación administrativa en beneficio de la ciudadanía.
v) El aumento de la recaudación del impuesto predial tomando como base el catastro actualizado.

El área de intervención del proyecto de acuerdo al estudio de pre inversión, prioriza 22 distritos que representan a 04 provincias (Chiclayo, Lambayeque, Lima Metropolitana y Piura) de 03 departamentos (Lambayeque, Piura y Lima) que a continuación se detalla:

REGIÓN LAMBAYEQUE

CIUDAD: CHICLAYO

DISTRITO	UNIDADES CATASTRALES
Chiclayo	95,221
José Leonardo Ortiz	55,231
La Victoria	25,373
Pimentel	11,446

CIUDAD: LAMBAYEQUE

DISTRITO	UNIDADES CATASTRALES
Lambayeque	18,761

REGIÓN: PIURA

CIUDAD: PIURA

DISTRITO	UNIDADES CATASTRALES
Piura (1)	98,783
Castilla	47,114
Catacaos	24,174
26 de Octubre	

(1) Proyección Incluye unidades catastrales del distrito 26 de Octubre

REGIÓN: LIMA

CIUDAD: LIMA

DISTRITO	UNIDADES CATASTRALES
Lima	139,158
Breña	39,991
Chorrillos	115,183
Comas	175,377
El Agustino	67,244
Independencia	76,107
Los Olivos	136,054
San Juan de Miraflores	129,088
San Luis	24,634
San Martin de Porres	228,570
San Miguel	60,668
Surquillo	43,629
Villa El Salvador	140,053

El número de unidades catastrales es un estimado al 2018 (Estudio de Preinversión)

5. OBJETIVOS

5.1 OBJETIVO GENERAL

El objetivo del servicio es contar con una infraestructura administrada a través de un proveedor de servicios de nube y administración de la misma, que soporte el desarrollo y funcionamiento del Sistema Catastral con un entorno adecuado para el funcionamiento de sus aplicaciones, networking, almacenamiento, software, capacidad de procesamiento y servicios de gestión para que los usuarios accedan a los recursos y servicios contratados.

El servicio a contratar comprende Servicio de Computación en la nube (Cloud Computing) en modalidad Infraestructura como servicio (IaaS), Plataforma como Servicio (PaaS) y Software como Servicio (SaaS) y en su mayoría se ha considerado los servicios Cloud en el modelo Paas por sus ventajas de flexibilidad para que los usuarios tengan control sobre las herramientas instaladas en la plataforma; adaptabilidad, movilidad y la velocidad, para potenciar el funcionamiento del Sistema Catastral.

El modelo PaaS (Platform as a Service) ofrece una variedad de características y servicios específicos que facilitan el desarrollo, la implementación y la gestión de aplicaciones en la nube como son: Entorno de desarrollo integrado, aprovisionamiento automático de recursos, gestión del ciclo de vida de una aplicación, escalabilidad automática, servicios de base de datos gestionados, integración con servicios externos, seguridad y cumplimiento, gestión y supervisión de recursos, despliegue continuo y automatización, pago por uso, facilita la colaboración, la escalabilidad geográfica. Características que facilitan el desarrollo y la gestión de aplicaciones en la nube, lo que permite a las empresas concentrarse en crear software de alto valor sin preocuparse por la gestión de la infraestructura subyacente.

Las ventajas de Plataforma como Servicio (PaaS) con relación a los gastos de capital y los gastos operativos son notables y potencialmente beneficiosas para la economía de una Entidad porque le permiten reducir tanto los gastos de capital como los operativos al eliminar la necesidad de invertir en hardware costoso, automatizar las tareas de administración, escalar eficientemente y beneficiarse de una facturación basada en el consumo. Esto da como resultado la optimización de los gastos y una mejor gestión de los recursos tecnológicos.

Una plataforma como servicios PaaS permite tener un menor costo de la inversión inicial, menos costos de mantenimiento y actualización de hardware, menor necesidad de espacio físico y energía. Asimismo, permite que la facturación sea basada en el uso, se puedan automatizar las tareas de gestión, aprovechar una escalabilidad eficiente, lograr mayor agilidad y eficiencia; y disminuir el personal especializado en infraestructura.

5.2 OBJETIVOS ESPECÍFICOS

Los objetivos específicos para la contratación son:

- Contar con los recursos necesarios o la capacidad tecnológica para el funcionamiento del Sistema Catastral.

- Contratar un proveedor de servicios de Cloud Computing en la modalidad de adquisición de recursos de manera flexible y con pagos mensuales en función de las cantidades de recursos que se utilicen en un ciclo de facturación mensual.
- El proveedor deberá presentar en su propuesta el monto total a contratar por el tiempo requerido. La Entidad pagará mes a mes solo los consumos que se realicen hasta consumir el monto total ofertado.
- El Postor deberá presentar en su propuesta el monto total a contratar por 12 meses. La Entidad contratará la solución de servicio de Plataforma en la Nube (PaaS) para el Sistema Catastral por 365 días calendarios o hasta alcanzar el consumo de la bolsa de créditos, pagando mensualmente lo que corresponda al ciclo de facturación y considerando los recursos consumidos.
- Aprovisionar infraestructura como servicio (IaaS) y plataforma como servicio (PaaS) de base de datos relacional y no relacional. El uso de Docker como una tecnología versátil para simplificar la gestión de aplicaciones, mejorar la eficiencia en el uso de recursos, facilitar la implementación y el mantenimiento de aplicaciones en diversos entornos. Aprovechando sus ventajas en términos de portabilidad, aislamiento, eficiencia y escalabilidad para modernizar y agilizar los procesos de administración de aplicaciones; así como el uso de Kubernets, una poderosa herramienta para la administración de contenedores y la orquestación de aplicaciones, que ofrece escalabilidad, alta disponibilidad y una amplia gama de características para simplificar la implementación y administración de aplicaciones en entornos de contenedores, aprovechando su flexibilidad y robusto ecosistema para aprovechar al máximo la tecnología de contenedores.
- Usar una arquitectura de microservicios basada en contenedores con una escalabilidad nativa y modular de la solución para el despliegue automatizado de las aplicaciones críticas y nuevos proyectos institucionales.
- Contar con mecanismos que permitan la capacidad de recuperación de los servicios de Catastro ante alguna situación de desastre (disaster recovery).
- Garantizar la disponibilidad continua de los servicios informáticos en producción de la UE 003 Cofopri.
- Brindar mecanismos de seguridad de la información alojada en la plataforma de nube.

6. ALCANCE DEL SERVICIO

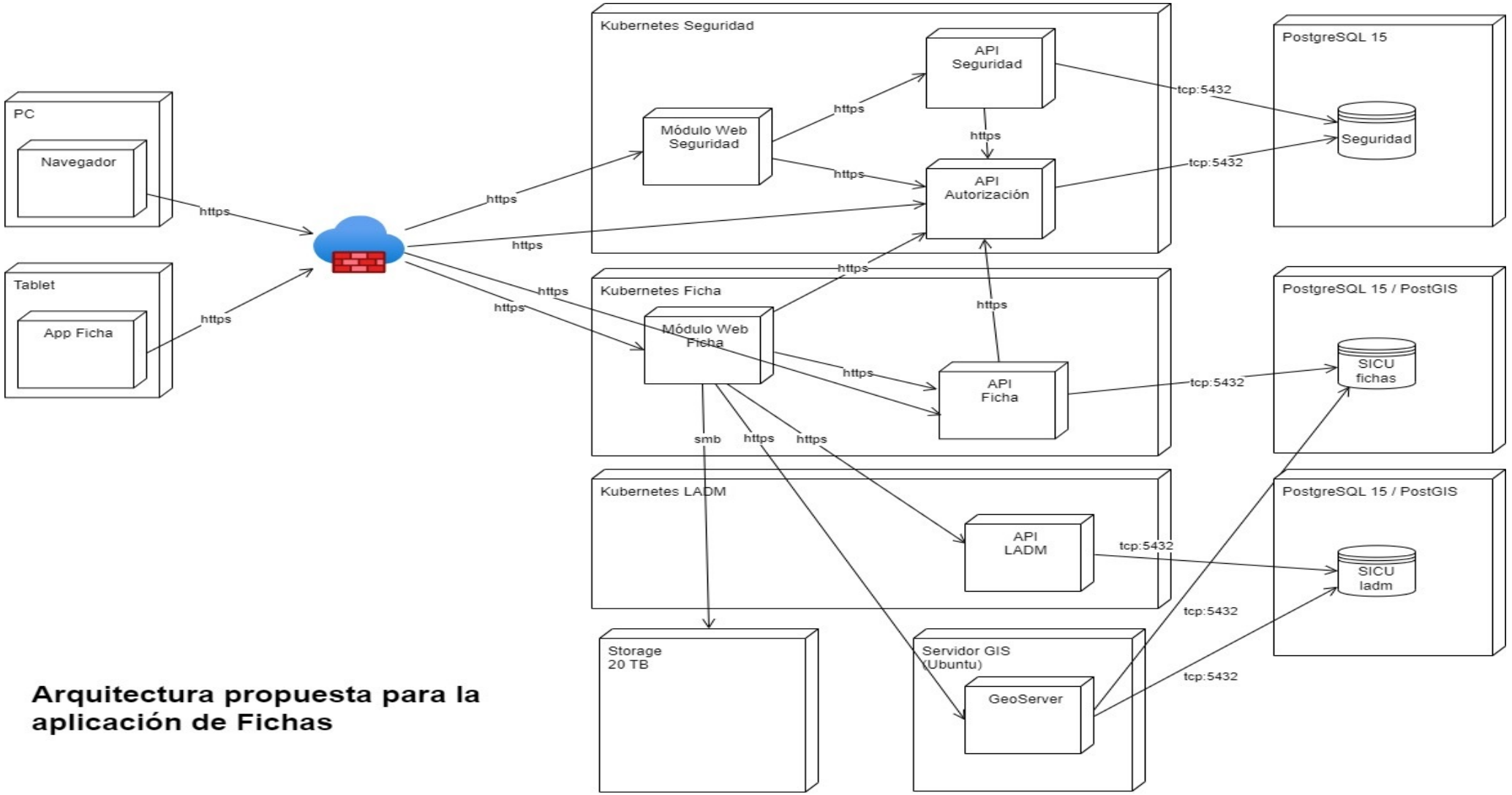
Servicio de Computación en la nube (Cloud Computing) en modalidad Infraestructura como servicio (IaaS), Plataforma como Servicio (PaaS) y Software como Servicio (SaaS) que permita a la UE 003 Cofopri tener los siguientes ambientes:

- Servicio de Clúster Kubernetes en donde se alojarán los contenedores y la aplicación de seguridad OAUTH2.
- Servicio de Clúster Kubernetes en donde se alojarán los contenedores y la aplicación de Ficha.
- Servicio de Clúster Kubernetes en donde se alojarán los contenedores y la aplicación de LADM Producción.
- Servidor GIS en donde se instalará GeoServer que permitirá ver y editar los datos geoespaciales.
- Servicio de infraestructura de almacenamiento de objetos en donde se alojará los archivos estáticos del sistema, como imágenes, fotos, pdf, etc.
- Servicios de base de datos PostgreSQL 15 en modalidad PaaS para almacenar las bases de datos de Seguridad, formularios de catastro urbano y LADM.

- Servicio de Web Application Firewall.
- Servicio de backup.

Todos los servicios requeridos en la infraestructura de la nube de internet (Cloud) deben ser brindados directamente por el fabricante Cloud que ofrece el contratista, siendo posible su configuración desde una única plataforma de administración. Los servicios y características que debe ofrecer el fabricante cloud ofertado por el contratista debe tener como mínimo lo siguiente:

Diagrama de Arquitectura de Producción



Arquitectura propuesta para la aplicación de Fichas

6.1 Disponibilidad global

- El servicio debe contar con centros de datos organizados por regiones, por lo menos cuatro regiones en el continente americano y cuatro en Europa.
- Los servicios de cómputo y almacenamiento deben permitir la selección de la región geográfica donde los servicios operen.
- El servicio debe permitir el despliegue para los servicios de cómputo en diferentes locaciones (centros de datos) dentro de la misma región elegida, con la finalidad que la Entidad pueda crear esquemas de continuidad de operaciones y recuperación en caso de desastre.
- El servicio debe asegurar que los datos sean almacenados única y exclusivamente en la región geográfica elegida salvo servicios que sean globales a la plataforma.

6.2 Administración de los servicios de nube

- La plataforma de nube debe proveer una consola de administración Web de todos los servicios en una misma consola de administración para todas las regiones.
- La plataforma debe tener la capacidad de conexión a través de una aplicación móvil (deseable)
- La plataforma debe proveer un SDK para interacción con los servicios
- La plataforma debe permitir la interacción a través de líneas de comando para interacción con los servicios
- La plataforma debe permitir la integración para configuración del envío de SMS a ejecutivos y administradores sobre el estado del servicio.

6.3 Experiencia del PSN

Debido a que el cumplimiento de los requisitos que la calidad y seguridad para las soluciones de COFOPRI depende directamente los servicios de Nube y por lo tanto del PSN, COFOPRI requiere que el mismo cumpla con los siguientes criterios:

- Deberá contar con las certificaciones del fabricante de proveedor de nube ofertado con las normas conocidas como ISO 9001, ISO 22301, ISO 27001, ISO 27017, ISO 27018 e ISO 27701. El postor del servicio podrá acreditar a través de link del fabricante, para ello se debe contar con la autorización o código para acceder a los certificados. Caso contrario deberá presentar copia simple de dichos certificados en su oferta.
- Debe tener disponibles en Internet los reportes de Control de Organización de Servicio SOC o presentar copia simple de dichos certificados en su oferta.
- CSA-STAR

6.4 Servicios de redes

- El servicio debe ser escalable y debe permitir especificar un rango de direcciones IP privadas de que sean elegidas.
- El servicio debe permitir ampliar la nube privada virtual mediante la incorporación de intervalos IP secundarios.
- 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.

- El servicio debe permitir controlar el acceso de entrada y salida desde y hacia subredes individuales por medio de listas de control de acceso.
- 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.
- El servicio debe permitir asignar varias direcciones IP y asociar múltiples interfaces de red elásticas a instancias de la nube privada virtual.
- 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.
- 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.
- El servicio debe permitir conectarse de manera privada y sin salir a internet a sus propios servicios o soluciones SaaS.
- El servicio debe permitir conectar la nube privada virtual y la infraestructura de TI local con la VPN del PSN de sitio a sitio.
- El servicio debe permitir asociar grupos de seguridad de la nube privada virtual con instancias en la plataforma.
- El servicio debe permitir habilitar IPv4 e IPv6 en la nube privada virtual.
- El servicio debe tener la habilidad de mover direcciones entre instancias
- El servicio debe tener la capacidad de análisis para monitoreo de tráfico de red.
- El servicio debe permitir implementar conectividad de tránsito (modelo Hub-andSpoke)
- El servicio debe permitir compartir una red virtual entre diferentes cuentas (modelo compartido)
- El servicio debe ofrecer resolución de DNS para entornos híbridos El servicio debe ofrecer resolución de DNS a nombres de host privados
- El servicio debe ofrecer resolución de DNS a nombres de host públicos
- NIC: el servicio debe contar con la capacidad para configurar comprobaciones de origen / destino en interfaces de red.

6.5 Servicio de Gestión de Identidad y Acceso

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

- El servicio debe permitir identificar cuándo se utilizó por última vez una clave de acceso para rotar claves antiguas.
- El servicio debe permitir establecer credenciales de seguridad temporales al realizar solicitudes entre servicios.

6.6 Servicio Entrega de Contenido (CDN)

El servicio de red rápido para entrega de Contenido debe permitir:

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

6.7 Servicio de instancias para cómputo

- El servicio debe contar con un auténtico 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 desee.
- El servicio debe permitir pausar y reanudar las instancias.
- El servicio debe contar con instancias de E/S de alto desempeño.
- El servicio debe contar con instancias de almacenamiento HDD denso.
- El servicio debe permitir configuraciones de CPU optimizadas
- El servicio debe contar con opciones de almacenamiento flexibles
- El servicio debe permitir hacer seguimiento de licencias para regular el uso y el cumplimiento
- El servicio debe permitir implementar funcionalidades de auto-escalamiento basadas en alarmas inteligentes.
- El servicio debe contar con la capacidad de sincronización de tiempo para instancias de cómputo.
- El servicio debe soportar acceso SSH basado en políticas
- El servicio debe ofrecer la posibilidad de colocar instancias en distintas regiones y zonas de disponibilidad
- El servicio debe permitir el uso de direcciones IP elásticas
- El servicio debe permitir ajustar la escala de la capacidad de las instancias automáticamente de acuerdo con las condiciones que se definan
- El servicio debe permitir acceder de manera privada a la API de las instancias desde su red privada de nube o sobre conexión directa, sin utilizar IP públicas y sin que el tráfico deba atravesar la Internet.
- Debe ofrecer un servicio de origen de hora de alta precisión, fiabilidad y disponibilidad que pueda ser usado por los servicios de cómputo.
- **El servicio debe contar con una disponibilidad mínima de 99,95%**

6.8 Servicio de Web Application Firewall

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

6.9 Servicio de base de datos relacional

- El servicio debe permitir automatizar las tareas administrativas, como el aprovisionamiento de hardware, la configuración de bases de datos, la implementación de parches y la creación de copias de seguridad. El servicio debe ofrecer varios tipos de recursos de cómputo: optimizados para memoria, rendimiento u operaciones de E/S
- El servicio debe ser compatible con herramientas para migrar o replicar las bases de datos existentes.
- El servicio debe estar en capacidad de encargarse de tareas habituales de las bases de datos, como el aprovisionamiento, las revisiones, las copias de seguridad, la recuperación, la detección de errores y la reparación.
- El servicio se debe poder desplegar en múltiples ubicaciones.
- El servicio debe permitir aplicar de forma automática parches de software.
- 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.
- El servicio debe ofrecer orientación sobre prácticas recomendadas mediante el análisis de las métricas de configuración y uso de los recursos de cómputo de bases de datos.
- El servicio debe ofrecer sugerencias sobre versiones de motores de base de datos, almacenamiento, tipos de recursos de cómputo y redes.
- El servicio debe permitir analizar las sugerencias disponibles y realizar una acción sugerida de inmediato, programarla para su próximo periodo de mantenimiento o descartarla por completo.
- El servicio debe contar con diversas opciones de almacenamiento en virtud del rendimiento requerido. Las opciones de almacenamiento deben incluir: Almacenamiento de uso general (SSD) y/o Almacenamiento de IOPS provisionadas (SSD).
- **El servicio debe permitir escalar los recursos informáticos y de memoria para ampliar o reducir la implementación, hasta un máximo de 32 vCPU y 244 GiB de RAM.**
- El servicio debe permitir aprovisionar almacenamiento adicional.

- El servicio debe permitir ampliar automáticamente el tamaño del volumen de la base de datos a medida que las necesidades de almacenamiento de la base de datos crecen, hasta un máximo de 64 TB o la cantidad máxima que establezca.
- El servicio debe permitir hacer réplicas de lectura.
- El servicio debe permitir crear una o varias réplicas de un recurso de cómputo de base de datos de origen determinada 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.
- El servicio debe permitir hacer copias de seguridad automatizadas. 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.
- El servicio debe permitir especificar el periodo de retención de copia de seguridad automática hasta un mínimo de 35 días calendarios culminados los 12 meses del servicio.
- El servicio debe permitir crear instantáneas de base de datos (copias de seguridad) que inicia el usuario de la instancia almacenada en el servicio de almacenamiento de objetos, y que se conservarán hasta que se eliminen explícitamente.
- El servicio debe permitir cifrar las bases de datos mediante las claves.
- 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.
- 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.
- 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.
- El servicio debe soportar la capacidad de notificar eventos de la base de datos por email o SMS
- 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.
- **El servicio debe soportar cifrado en reposo con claves administradas por COFOPRI.**
- **El servicio debe contar con capacidad de conmutación por error (automatizada)**
- **El servicio debe contar con capacidad de prueba de conmutación por error (manual)**
- El servicio debe soportar leer réplicas, replicación retrasada (para configuraciones de recuperación ante desastres.
- El servicio debe soportar escalamiento horizontal.

6.10 Servicio de Balanceador de carga

- El servicio debe distribuir automáticamente el tráfico de aplicaciones entrantes a través de varios destinos, tales como instancias y direcciones IP.
- 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.
- Se deben poder crear y administrar grupos de seguridad asociados con balanceadores de carga a fin de ofrecer opciones de seguridad y redes adicionales
- 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.

- El servicio debe permitir equilibrar cargas de trabajo a nivel de capa 4 y capa 7.
- El servicio debe permitir equilibrar la carga en aplicaciones HTTP o HTTPS para características específicas de la capa 7.
- El servicio debe facilitar el monitoreo de rendimiento de las aplicaciones en tiempo real.
- **El servicio debe proporcionar direccionamiento de solicitudes avanzado destinado a la entrega de arquitecturas de aplicaciones modernas, incluidos micro servicios y aplicaciones basadas en contenedores.**
- El servicio debe asegurar que se utilicen en todo momento los protocolos y cifradores SSL/TLS más recientes.
- El servicio debe poder presentar varios certificados mediante el mismo agente de escucha seguro, lo que le permite admitir varios sitios web seguros a través del uso de un único agente de escucha seguro.
- Cuando el nombre de host indicado por un cliente coincide con varios certificados, el servicio debe estar en capacidad de establecer cuál es el certificado más adecuado en función de varios factores, entre ellos, las capacidades del cliente.
- El servicio debe permitir distribuir el tráfico de entrada entre destinos en numerosas zonas de disponibilidad.
- El servicio debe escalar automáticamente la capacidad de administración de solicitudes como respuesta al tráfico de aplicaciones entrante.
- El servicio debe soportar: direccionamiento basado en host, direccionamiento basado en ruta, direccionamiento basado en el encabezado HTTP, direccionamiento basado en el método HTTP, direccionamiento basado en parámetros de cadenas de consultas y direccionamiento basado en CIDR para direcciones IP de origen.
- El servicio debe poder direccionar una solicitud de cliente basada en el CIDR para direcciones IP de origen desde donde se origina la solicitud.
- El servicio debe ser compatible con HTTP/2.

6.11 Servicio para Monitorización y Observación

Deberá contarse con un servicio de monitoreo ya sea propietario o terceros, que permita:

- Ofrecer datos e información procesable para monitorear las aplicaciones.
- Permita a través de los datos responder a los cambios de rendimiento que afectan al sistema
- Presenta información para optimizar el uso de recursos y una vista unificada de estados de operaciones.
- Recopilar datos de monitorización en formatos de registros, métricas y eventos.
- Tener una consola de vista Unificada de recursos, aplicaciones y servicios que se ejecuten en los servidores desplegados por COFOPRI

6.12 Servicio para Auditoría y Gobernanza

Deberá contarse con un servicio para la auditoría de conformidad operativa y de riesgo en la cuenta que permita:

- Registrar, monitorear de manera continua y retener la actividad de la cuenta cloud relacionada con acciones en toda la infraestructura.
- Proporcionar el historial de los eventos de actividad de la cuenta.

- Registrar las acciones efectuadas sobre la cuenta ya sea a través de una consola, clientes de conexión, línea de comandos y otros servicios de operación para los recursos.
- Simplificar el análisis de seguridad, seguimiento a cambios en los recursos y resolución de problemas sobre los servicios.
- Detectar actividad inusual en los recursos

6.13 Capacidad de medición de servicios de transferencia

El servicio de gestión de infraestructura deberá tener capacidades para:

- Identificar y medir el tráfico de datos desde, hacia y dentro de la nube.
- Identificar los costos asociados a dicho tráfico.

6.14 Servicio de Gestión de Backups

COFOPRI requiere que el contratista cuente con un servicio de Backup que permita:

- Proveer la infraestructura necesaria para realización de los backups requeridos por COFOPRI
- COFOPRI Proporcionará un listado de las aplicaciones y bases de datos respectivamente a las cuales se deberá tener como foco de configuración para la toma de backups.

6.15 Servicio de escalado de aplicaciones para optimizar los costos y el nivel de desempeño

- El servicio debe permitir lanzar y finalizar recursos de cómputo.
- El servicio debe poder escanear el entorno y descubrir automáticamente los recursos escalables en la nube subyacentes a la aplicación, por lo que no se requiere identificar manualmente estos recursos uno por uno a través de interfaces de servicio individuales.
- El servicio debe permitir seleccionar políticas específicas para incrementar o reducir instancias de manera horizontal de forma que se llegue a cubrir la demanda necesaria
- El servicio debe permitir implementar estrategias de escalamiento predictivo a partir del tráfico futuro, incluidos los picos que ocurren regularmente, y aprovisiona el número correcto de recursos de cómputo antes de los cambios previstos. Utilizando algoritmos de aprendizaje automático
- El servicio debe permitir crear automáticamente políticas de escalado de seguimiento de destino para todos los recursos del plan de escalado
- El servicio debe poder calcular continuamente los ajustes de escala apropiados e inmediatamente debe agregar y eliminar capacidad según sea necesario para mantener las métricas en el objetivo. El servicio debe permitir que las políticas de escalado de seguimiento de objetivos se optimicen automáticamente y aprendan sus patrones de carga reales para minimizar las fluctuaciones en la capacidad de los recursos.
- El servicio debe tener la capacidad de realizar acciones personalizadas en recursos de cómputo que se inician / finalizan
- El servicio debe ofrecer la posibilidad de personalizar las políticas de escalado.
- El servicio debe permitir habilitar y deshabilitar las políticas de escalado
- El servicio debe permitir marcar un recurso de cómputo en mal estado para programar su reemplazo
- El servicio debe permitir utilizar AMI (o imágenes de la galería) para aprovisionar instancias / máquinas virtuales en un grupo de escalado.

6.16 Servicio de Almacenamiento de objetos

- El servicio debe contar con capacidades para anexar etiquetas de metadatos a los objetos, mover y almacenar datos entre los tipos de almacenamiento, configurar y aplicar controles de acceso a datos, proteger los datos frente a usuarios no autorizados, ejecutar análisis de big data y monitorear los datos en los niveles de objeto y carpetas que contienen objetos.
- El servicio debe permitir el acceso a los objetos a través de los puntos de acceso del servicio o directamente a través del nombre de host de la carpeta que los almacena.
- El servicio debe permitir utilizar un informe de inventario, donde se enumeran los objetos almacenados en una carpeta de objetos o con un prefijo específico, así como sus metadatos y estado de cifrado correspondientes.
- 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.
- El servicio debe admitir características que ayudan a mantener el control de versiones de los datos, impedir el borrado accidental y replicar datos en diversas ubicaciones del PSN.
- 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.
- El servicio debe permitir replicar objetos (así como sus metadatos y etiquetas de objeto respectivos) en otras regiones del PSN o en la misma ubicación para lograr una latencia reducida, conformidad, seguridad y recuperación de desastres.
- El servicio debe permitir aplicar políticas de escritura única y lectura múltiple (WORM)
- El servicio debe permitir aplicar etiquetas a las carpetas para asignar costos en múltiples dimensiones de negocio (por ejemplo, centros de costos, nombres de aplicación o propietarios) y, después, debe permitir utilizar los informes de asignación de costos para ver el uso y los costos que agregan las etiquetas de las carpetas.
- El servicio debe permitir hacer el seguimiento de las actividades de nivel de carpetas y objeto e informar sobre ellas.
- El servicio debe permitir crear usuarios y administrar su correspondiente acceso.
- El servicio debe conceder acceso a objetos individuales a los usuarios autorizados
- El servicio debe permitir configurar permisos para todos los objetos de una única carpeta.
- El servicio debe permitir simplificar la administración del acceso de datos a conjuntos de datos compartidos creando puntos de acceso con nombres y permisos específicos para cada aplicación o conjuntos de aplicaciones
- El servicio debe conceder acceso a otros usuarios por tiempo limitado con direcciones URL temporales.
- El servicio debe ofrecer características de seguridad flexibles para bloquear el acceso de usuarios no autorizados a sus datos
- El servicio debe admitir el cifrado tanto del lado de servidor (con tres opciones de administración clave) como del lado de cliente para cargas de datos.
- El servicio debe contar con controles de seguridad que garantizan que las carpetas y objetos no tengan acceso público
- El servicio debe contar con clases de almacenamiento: clase / nivel de almacenamiento de movimiento de datos automático basado en patrones de acceso

6.17 Consideraciones de Seguridad

6.17.1 Seguridad de la infraestructura

La nube debe ofrecer varias capacidades y servicios de seguridad para aumentar la privacidad y controlar el acceso a la red. Estos deben incluir lo siguiente:

- La nube debe permitir crear redes privadas y controlar el acceso a sus recursos de cómputo o aplicaciones.
- COFOPRI debe poder controlar el cifrado en tránsito con TLS a través de los servicios de la nube.
- La nube debe ofrecer opciones de conectividad que permitan conexiones privadas o dedicadas desde COFOPRI .
- La nube debe contar con tecnologías de mitigación de DDoS que se aplican en la capa 3 o 4, así como en la capa 7.
- La nube debe contar con la capacidad de aceptar el cifrado de todo tráfico.

6.17.2 Servicio de Cifrado de datos

La nube debe ofrecer la posibilidad de agregar una capa de seguridad a los datos en reposo, proporcionando funciones de cifrado escalables y eficientes. Estos deben incluir lo siguiente:

- La nube debe contar con capacidades de cifrado de datos en reposo en los servicios requeridos por COFOPRI
- La nube debe contar con opciones flexibles de administración de claves, incluido un servicio de administración de claves propio de la nube.

6.17.3 Control de Identidad y Acceso

La nube debe ofrecer capacidades para definir, hacer cumplir y administrar las políticas de acceso de los usuarios en todos los servicios. Estos deben incluir lo siguiente:

- La nube debe contar con un servicio que le permita a COFOPRI definir cuentas de usuario individuales con permisos en todos los recursos de la nube.
- La nube debe contar con autenticación multi-factor para cuentas privilegiadas, incluidas opciones para autenticadores basados en software y hardware.
- La nube debe contar con un servicio que permita otorgar a los funcionarios de COFOPRI y a las aplicaciones acceso federado a la consola de administración.
- La nube debe contar con inicio de sesión único (SSO) que le permita a COFOPRI administrar el acceso SSO y los permisos de usuario a todas sus cuentas de la nube de manera centralizada.

6.17.4 Monitoreo y Registro

La nube debe proporcionar herramientas y características que le permitan a COFOPRI ver lo que sucede en su entorno de nube. Estos deben incluir lo siguiente:

- La nube debe contar con un servicio que permita monitorear las implementaciones en la nube al obtener un historial de llamadas API para la cuenta de COFOPRI
- La nube debe permitir identificar qué usuarios y cuentas llamaron API de la nube para los servicios que admiten esta funcionalidad. En particular debe permitir hacer seguimiento de la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron las llamadas.

- La nube debe contar con una solución de monitoreo confiable, escalable y flexible
- La nube debe contar con un servicio de detección de amenazas que monitorea continuamente la actividad maliciosa y el comportamiento no autorizado para proteger la cuenta de COFOPRI y cargas de trabajo que este ejecutando por COFOPRI en la nube.
- La nube debe exponer las notificaciones para que pueda activar una respuesta automatizada o notificar a la persona designada por COFOPRI.
- La nube debe contar con herramientas y características que den visibilidad a COFOPRI para detectar problemas antes de que afecten el desarrollo de las actividades soportadas por la nube y permitan mejorar la postura de seguridad y reducir el perfil de riesgo.

6.18 Optimización de Arquitectura

El postor deberá proponer una arquitectura en la que incorpore las siguientes buenas prácticas de diseño:

6.18.1 Escalabilidad

Se espera que los sistemas de COFOPRI crezcan con el tiempo y por lo tanto deben construirse sobre una arquitectura escalable. Dicha arquitectura debe soportar el crecimiento de usuarios, tráfico o tamaño de datos. El escalamiento debe poder hacerse de forma horizontal y vertical.

6.18.2 Administrar Volúmenes Crecientes de Datos

Para la administración de grandes volúmenes crecientes de datos se debe implementar una arquitectura de lago de datos cuando sea necesario y posible.

- Eliminar puntos únicos de falla: La arquitectura debe soportar la falla de un componente individual o de múltiples componentes, como discos duros, servidores y enlaces de red. Para tal fin se deben implementar sistemas con alta disponibilidad o establecer formas de automatizar la recuperación y reducir las interrupciones en cada capa de su arquitectura cuando sea necesario y posible.
- Redundancia: Cuando sea necesario y posible se debe incluir redundancia en los componentes de nube; es decir, se debe contar con múltiples recursos para la misma tarea. La redundancia se puede implementar en modo de espera o activo según la necesidad.
- Detección de fallas: Cuando sea necesario y posible se debe construir la mayor automatización viable tanto en la detección como en la reacción ante fallas.
- Almacenamiento de datos duradero: Cuando sea necesario y posible la arquitectura debe proteger tanto la disponibilidad como la integridad de los datos.
- Resiliencia automatizada de múltiples centros de datos: Las aplicaciones críticas para el negocio deben contar con protección contra escenarios de interrupción con una baja probabilidad, pero un gran riesgo de impacto, como una catástrofe natural que derriba toda la infraestructura durante mucho tiempo. En tales casos, la arquitectura debe contar con esquemas de resiliencia automatizada en múltiples centros de datos.

6.18.3 Optimización de Costos

Mediante una metodología iterativa se deben crear arquitecturas con costos optimizados usando los siguientes principios de diseño:

- Tamaño correcto: se debe comparar el entorno de la aplicación y seleccionar el tipo de servicio en la nube correcto; es decir, dependiendo de cómo es la carga de trabajo se debe seleccionar la CPU, RAM, red, tamaño de almacenamiento, E/S, etc. apropiados.
- Aprovechamiento de las opciones de compra: Se debe seleccionar las opciones de compra más costo-efectivas disponibles para la adquisición de los recursos de nube.

7. DESCRIPCIÓN DEL SERVICIO

El Servicio de Nube para el Sistema Catastral debe comprender los siguientes servicios:

7.1 Servicio de Cloud Computing

El servicio de alojamiento de servidores y servicios en nube pública debe entregarnos el servicio de Cloud Computing (PaaS, IaaS y SaaS), con sus capacidades de procesamiento, almacenamiento, comunicaciones y operaciones para los entornos de Producción de las aplicaciones del Sistema Catastral. A su vez, el servicio debe proveer las capacidades (infraestructura, capacidades de procesamiento, almacenamiento, redes) necesarias para brindar el acceso a los usuarios de los sistemas y aplicaciones con capacidad de recuperación ante un desastre.

Con el fin de realizar el cálculo del costo del servicio, el proveedor deberá tomar únicamente en consideración las características que a continuación se detallan, entendiéndose que estas son referenciales y no necesariamente deberán ser instaladas o ponerse en servicio a la firma del Contrato. Deben considerarse sólo para efectos de estimación de costo de la bolsa de capacidades a contratar.

El CONTRATISTA deberá considerar como mínimo los siguientes recursos computacionales, los cuales serán usados al 100% de su capacidad y en Alta Disponibilidad:

ESPECIFICACIONES TÉCNICAS:

Ítem	Componente	Descripción	Detalle	Ambiente	Cantidad
1	Kubernetes Seguridad	Servicio de Clúster Kubernetes en donde se alojarán los contenedores y la aplicación de seguridad.	Versión: 1.27 (como mínimo) Nodos: 3 como mínimo Máximo: de acuerdo a la demanda vCPU: 4 RAM: 8 GB Storage: 50 GB Otros: Alta Disponibilidad Rendimiento de red de los Nodos: 10gbps	Producción	01
2	Kubernetes Ficha	Servicio de Clúster Kubernetes en donde se alojarán los contenedores y la aplicación de Ficha.	Versión: 1.27 (como mínimo) Nodos: 3 como mínimo Máximo: de acuerdo a la demanda vCPU: 4 RAM: 8 GB	Producción	01

Ítem	Componente	Descripción	Detalle	Ambiente	Cantidad
			Storage: 50 GB Otros: Alta Disponibilidad Rendimiento de red de los Nodos: 10gbps		
3	Kubernetes LADM Producción	Servicio de Clúster Kubernetes en donde se alojarán los contenedores de aplicación web y LADM.	Versión: 1.27 (como mínimo) Nodos: 3 como mínimo Máximo: de acuerdo a la demanda vCPU: 4 RAM: 8 GB Storage: 50 GB Otros: Alta Disponibilidad Rendimiento de red de los Nodos: 10gbps	Producción	01
4	Servidor GIS	Servidor GIS en donde se instalará GeoServer que permitirá ver y editar los datos geoespaciales.	Configuración mínima: vCPU: 2 RAM: 8 GB Storage: 20 GB Configuración máxima vCPU: 4 RAM: 16 GB Storage: 512 GB S.O.: Ubuntu Server / GeoServer Otros: Alta Disponibilidad	Producción	01
5	File Storage (Almacenamiento)	Servicio de Storage en donde se alojan los archivos estáticos del sistema, como imágenes, fotos, pdf, etc. Standard storage (20 TB/mes)	Storage: Mínimo: 1 TB Máximo: 20 TB Otros: Alta Disponibilidad	Producción	01
6	PostgreSQL 15 Seguridad	Servicio de base de datos de tipo PostgreSQL 15 para almacenar la base de datos de Seguridad.	Mínimo: vCPU: 2 CPU RAM: 4 GB Storage: 20 GB Máximo vCPU: 4 CPU RAM: 16 GB Storage: 512 GB Alta disponibilidad Multirregión Motor: PostgreSQL Versión 15 (como mínimo)	Producción	01
7	PostgreSQL 15 Ficha	Servicio de base de datos de tipo PostgreSQL 15 con	Mínimo: vCPU: 2 CPU RAM: 4 GB	Producción	01

Ítem	Componente	Descripción	Detalle	Ambiente	Cantidad
		PostGIS para almacenar la base de datos de Ficha.	Storage: 20 GB Máximo: vCPU: 6 CPU RAM: 24 GB Storage: 5 TB Alta disponibilidad Multirregión Motor: PostgreSQL Versión: 15 (como mínimo) con PostGIS		
8	PostgreSQL 15 LADM	Servicio de base de datos de tipo PostgreSQL 15 con PostGIS para almacenar la base de datos LADM.	Mínimo: vCPU: 2 CPU RAM: 4 GB Storage: 20 GB Máximo: vCPU: 4 CPU RAM: 8 GB Storage: 500 GB Alta disponibilidad Multirregión Motor: PostgreSQL Versión: 15 (como mínimo)	Producción	01
9	Servicio de redes - Puerta de enlace para direcciones de red		500 GB cada uno	Producción	02
10	Servicio de red de entrega de contenido		Transferencia saliente a internet: 1024GB/mes Transferencia saliente a origen: 1024GB/mes		
11	Servicio de Balanceador de Carga		Datos procesados 1024 GB/mes		
12	Servicio de monitorización y observación		Cantidad de métricas: 42 Registros: 50GB		
13	Servicio de Firewall		Número de reglas por ACL: 15		
14	Servicio de protección de actividades maliciosas		Para almacenamiento Clústers Servidor GIS Bases de datos		
15	Servicio de Backup		Almacenamiento para instancias de cómputo: 20TB Retención de copia de seguridad diario: 7 Retención de copia de seguridad semanal: 4		

● El servicio debería contar con un repositorio de imágenes contenerizadas
● Deberá contar con un portal de autoaprovisionamiento por el cual la entidad podrá acceder a los servicios requeridos. Este portal de aprovisionamiento debe ser protegido por un mecanismo de doble autenticación, además de usuario y contraseña.
● Deberá contar con un servicio que permita gestionar el control de los accesos e identidades de los usuarios a la cuenta de nube pública otorgada. Permitirá a la entidad gestionar cuentas de usuario y autorizar permisos para los recursos de la nube pública.
● Las capacidades de cómputo podrán reducirse o detenerse en horarios en los cuales no se tenga mucha demanda o acceso hacia las soluciones; asimismo, podrán aumentarse las capacidades de cómputo de ser necesario, de manera que los Usuarios no se vean afectados y la UE003 COFOPRI pueda optimizar los recursos contratados.
● El servicio debe soportar los Sistemas Operativos requeridos en sus diferentes versiones y distribuciones cómo mínimo Microsoft Windows y Linux.

● Las licencias del Sistema Operativo serán asumidas por el CONTRATISTA.
● Las capacidades de cómputo solicitadas podrán aumentarse en base a la demanda de usuarios que accedan a los servicios alojados en la nube, a través de un servicio de auto escalado de la plataforma cloud.
● Debe ser un servicio escalable de acuerdo con las necesidades que se requiera, para el funcionamiento del sistema catastral y en base a las condiciones de los recursos contratados de acuerdo con el servicio de nube pública.
● Debe contar con un portal de autoaprovisionamiento por el cual LA ENTIDAD podrá acceder a los servicios requeridos con un usuario y contraseña.
● Debe contar con un servicio que permita gestionar el control de los accesos e identidades de los usuarios a la cuenta de nube pública otorgada. Permitirá a LA ENTIDAD gestionar cuentas de usuario y autorizar permisos para los recursos de la nube pública.
● Debe contar con la provisión de servicios Infraestructura como servicio (IaaS), Plataforma como Servicio (PaaS) y/o Software como servicios (SaaS).
● Deberá poder orquestar la tecnología de contenedores con sus versiones estables.
● Deberá soportar imágenes de contenedor en formato Docker.
● Deberá soportar la portabilidad de las aplicaciones permitiéndoles ser movidos y alojados fuera de la plataforma de nube privada.
● Deberá permitir la integración con un controlador de versiones ya sea en forma nativa o por medio de una herramienta de integración continua y/o entrega continua.
● Deberá ser capaz de integrarse con herramientas de integración y entrega continua tales como Jenkins.
● El enrutamiento y balanceo de tráfico podrá ser una funcionalidad propia de la plataforma de contenedores.
● Deberá permitir detectar auto problemas con los nodos que no respondan y reemplazarlos de forma automática con un nuevo nodo e incluirlo al clúster de Kubernetes.
● Deberá contar con un mecanismo para reiniciar los PODs/Containers que tengan problemas.
● Permitir Upgrade de manera granular: un nodo a la vez, de forma automática, con rollback automático en caso de problemas.
● Debe permitir descargar las máquinas virtuales o imágenes en caso se requiera.
● La plataforma deberá incluir el servicio de despliegue de base de datos relacionales que permita desplegar cualquier de las siguientes bases de datos: PostgreSQL
● Debe contar con un servicio de alarmas. Estas alarmas podrán utilizarse para recopilar y seguir métricas, definir alarmas y reaccionar de modo automático ante los cambios en sus recursos. Estas alarmas revisarán el estado de los servicios de cómputo, almacenamiento, balanceo de carga. Estos servicios deberán estar disponibles desde el portal de autoaprovisionamiento y permitirán conocer el estado de funcionamiento y el rendimiento de los objetos monitorizados de cada servicio, en tiempo real.
● Debe incluir el provisionamiento de direcciones IP públicas a demanda desde el mismo portal de autoaprovisionamiento, que permitirá la publicación de las aplicaciones por internet.
● La operación de comunicación por IP Pública estará disponible de forma permanente (24 horas del día, los 365 días al año), con un SLA de disponibilidad mínima de comunicación de 99.95%.
● La solución WAF podrá ser brindada por la nube pública como un servicio nativo, con la finalidad de brindar seguridad a los servicios web ante violaciones de protocolos inferiores al aplicativo, incluyendo inyección de inspección de paquetes “http”. Deberá detectar, alertar y bloquear, en tiempo real cualquier comportamiento malicioso conocido y/o desconocido. Deberá bloquear las transacciones web en forma preventiva, antes de que estas lleguen vía red a los servidores. Deberá soportar diferentes políticas que se asocien a las aplicaciones web. Deberá tomar acciones adecuadas ante algún ataque o alguna otra actividad no autorizada como mínimo. Asimismo, se podrán extender capacidades para proteger entornos cloud como OnPremise. Debe permitir crear reglas para filtrar las solicitudes web en función de condiciones como la dirección IP, los encabezados y cuerpos HTTP o los URI personalizados
● La infraestructura como servicio debe incluir un servicio de respaldo basado en snapshots que permita respaldar los discos de las máquinas virtuales usando políticas de respaldo.
● El servicio de backup no deberá necesitar de la instalación de agentes en el ambiente o máquinas virtuales para poder realizar sus tareas de respaldo y recuperación de máquinas virtuales.
● La solución de nube pública debe contar con el servicio de “autoescalado” para gestionar el crecimiento en base a la demanda de recursos de cómputo.
● El servicio deberá permitir realizar tareas de autoescalado basado en alarmas.

● El servicio deberá permitir realizar el autoescalado para ajustar los anchos de banda a intervalos programados, una hora específica o como alarmas activadas.
● El servicio deberá permitir cambiar las redes virtuales VPC de los servidores en caliente, manteniendo la continuidad de las operaciones.
● Las direcciones IP privadas se pueden especificar durante la creación de un recurso de cómputo. Las direcciones IP son consecutivas si las instancias se crean en un lote.
● El servicio deberá permitir aumentar el ancho de banda de las IPs públicas en caliente sin interrumpir el servicio.
● Debe permitir realizar el incremento o reducción de capacidades de estas máquinas virtuales, de acuerdo con los requerimientos iniciales.
● La solución de nube pública ofertada deberá tener un nivel de disponibilidad mínimo de 99.95% mensual para el servicio de cómputo.
● El servicio de soporte ante incidencias será en la modalidad 24x7 y deberá ser prestado en idioma español directamente por el proveedor de la solución de nube pública. En el caso se requiera de soporte altamente especializado (nivel 3), este podrá ser ofrecido en inglés y la atención del mismo podrá realizarse de manera remota.

7.2 Software Base

● El CONTRATISTA proveerá el servicio base necesario para la implementación de cada componente de las aplicaciones provistas por la Unidad Ejecutora 003. El servicio base deberá incluir como mínimo el Sistema Operativo y servicios estándares de la plataforma de nube, en caso de que se requiera.
● El CONTRATISTA para todos los ambientes en cada sistema, será responsable del licenciamiento, mantenimiento, ejecución de actualizaciones y soporte de los servicios base brindado.
● La Unidad Ejecutora 003 será responsable de proveer las licencias de los Sistemas y Aplicaciones u otro software necesario, como los certificados SSL, para el correcto funcionamiento de las aplicaciones y/o servicios de la Entidad.

8. DE LA IMPLEMENTACIÓN

La implementación será ejecutada por el CONTRATISTA (Partner del Proveedor de Servicios Cloud) y la Unidad Ejecutora 003 Cofopri, de manera conjunta y coordinada. La implementación se ejecutará en un plazo de hasta treinta (30) días calendario, a partir del día siguiente de la firma de contrato. Las actividades incluirán:

- Configuración y despliegue de la plataforma Cloud Computing.
- Los trabajos podrán realizarse tanto en días laborables y no laborables. No laborables previa coordinación entre las partes.
- Los trabajos deben ser ejecutados por personal debidamente certificado en la plataforma de nube pública ofertada.

9. DISEÑO DEL SERVICIO

El servicio de Cloud Computing deberá brindar al Sistema Catastral las capacidades bajo demanda, que permitan la creación de servicios y máquinas virtuales; y reporte del estado de los servicios.

El proveedor brindará la consola de medición y control del servicio, con el fin de medir el consumo y calidad del servicio brindado. Tener en cuenta que en esta consola los administradores podrán configurar alertas del consumo de datos correspondiente a la bolsa contratada. Las alertas deberán ser configuradas por el proveedor integral en coordinación con el Especialista de Sistemas y Tecnologías de la UE003

Deberá estar conformada por un modelo de aprovisionamiento que cuente con los siguientes elementos:

9.1 Conectividad a los Servicios en la nube

- La red virtual deberá permitir crear redes y subredes privadas virtuales en donde se desplegarán los servicios y máquinas virtuales.

- Todo acceso hacia el servicio de las plataformas de la nube debe utilizar protocolos seguros haciendo uso de certificados SSL, con llaves de encriptación de 256 bits como mínimo.

- Garantizar un tráfico interno de hasta 10 Gbps por instancia de los distintos componentes en la nube.

- La Infraestructura de Servidores a proveer por El CONTRATISTA deberá interconectarse con la Sede Principal del Sistema Catastral usando para ello una conexión VPN Ipsec *Site-to-site* que será configurada sobre un enlace a Internet provisto por la Unidad Ejecutora 003.

- En la infraestructura del CONTRATISTA deberá implementarse una salida a Internet para publicar los servicios y aplicaciones, para lo cual se debe considerar el aprovisionamiento de direcciones IP públicas.

9.2 Monitoreo de la Infraestructura y servicios cloud

El portal de monitoreo de la solución contará con las siguientes funcionalidades:

- Estar disponible 24x7x365
- Proveer las herramientas para realizar el monitoreo, alertas de consumo y visualizar los siguientes aspectos:
    - Monitoreo de los recursos computacionales (Uso de CPU, memoria, espacio discos, tráfico de red entrante y saliente).
    - Transferencia de datos mensual.
- El servicio de monitoreo debe permitir generar reportes mensuales descargables de todos los recursos de infraestructura que correspondan al ambiente de Producción.

9.3 Servicio de Respaldos y backup

El servicio de respaldos de constar principalmente:

- Respaldo de máquinas virtuales contemplando lo siguiente:
    - Debe estar basado en tecnología de snapshots y debe permitir el respaldo consistente de varios discos montados para restaurar la información de una máquina virtual.
    - Debe permitir el uso de una política de backup incluyendo nombre, tiempo de ejecución, periodo de retención. Las políticas permitirán asociar máquinas virtuales para ser ejecutadas de manera automática.
    - Debe permitir respaldos periódicos y a demanda.

- El servicio debe permitir automatizar los trabajos de copia de seguridad y recuperación a nivel de recursos de cómputo sin la necesidad de scripts personalizados o soluciones de terceros.
- El servicio debe tener la capacidad para crear políticas de respaldo que abarquen múltiples recursos y servicios.

▪ Respaldo de archivos y base de datos usando una solución, que deberá contemplar lo siguiente:
- Se ejecutará pruebas de respaldo y restauración.
- El servicio deberá contar con un Backup de los ambientes virtuales y de la data almacenada, la cual deberá definirse en conjunto con el proveedor de servicios en base a los recursos contratados. De requerir incrementales en el tiempo sobre la línea base contratada, serán contratados como adicionales.

9.4 Seguridad

- La solución deberá contar con mecanismos de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información.
- Para los servidores desplegados en la nube se usarán grupos de seguridad para el filtrado de tráfico entrante y saliente.
- Para las aplicaciones web, el PROVEEDOR deberá proporcionar protección contra ataques web a través del servicio de Firewall de aplicaciones web.
- El servicio de Firewall de Aplicaciones Web deberá como mínimo mitigar riesgos de seguridad de OWASP Top 10.

9.5 Esquema de Contingencia

- El CONTRATISTA deberá proporcionar para el presente servicio, al menos dos (02) Centros de Cómputo, geográficamente separados para albergar la infraestructura a proveer.
- El CONTRATISTA deberá considerar en el diseño de la infraestructura la distribución de los recursos computacionales en al menos dos (02) Centros de Cómputo.
- Los centros de cómputo deberán contar con certificación Tier 3 o superior.

9.6 Centros de Cómputo

Los Centros de Cómputo del proveedor del servicio deben cumplir con un mínimo de características en los 3 siguientes principios: Escalabilidad, Disponibilidad y Seguridad.

- **Escalabilidad**, contará con una plataforma que permita crecimientos de capacidad de procesamiento y almacenamiento: indicar si es escalable en forma horizontal (a través de varios servidores), vertical (crecimiento a equipos más grandes o con más equipamiento) o ambas características.

- **Disponibilidad**, Deberá proveer el servicio garantizando la continuidad operacional durante el período duración del Servicio.

- **Seguridad**, Deberá proveer el servicio desde los Centros de Computo que cuente con la infraestructura, normas y procedimientos de seguridad, mecanismos físicos y lógicos necesarios mínimos implementados y componentes que permitan maximizar su disponibilidad.

9.7 Definición de SLA de Soporte

En esta sección se define la criticidad de los incidentes y el tiempo de respuesta que debe ofrecer el CONTRATISTA para cada caso.

Urgente: los sistemas no pueden funcionar y los usuarios están imposibilitados de trabajar (producción está caído).

Alta: los sistemas en producción presentan fallas en su funcionamiento, pero hay partes de estos que se pueden utilizar sin ningún tipo de inconvenientes y no representan un riesgo en su uso. Sin embargo, hay partes del sistema que, o bien no se puede ingresar o tienen algún tipo de mal funcionamiento que podrían provocar eventuales problemas de alguna índole a los servicios en producción. En resumen, si hay algo que afecta la operatividad en producción.

Normal: el sistema puede presentar eventuales inestabilidades debido a que algunas partes de los sistemas dependen de la actualización de algún componente de toda la plataforma. O bien, de común acuerdo se clasifica el evento como no crítico debido a que por su naturaleza no representa un elevado riesgo para el correcto funcionamiento de los sistemas. Necesario, pero no afecta la operatividad en producción.

Baja: los incidentes que no entren en las categorías anteriores.

Tratamiento de eventos de prioridad "Urgente": ante la ocurrencia de un evento de esta naturaleza, el CONTRATISTA se compromete a brindar la atención "remota" en un plazo no superior a las 2 horas laborales de haber recibido la comunicación correspondiente, por parte de la UE003, los días laborables de 9 a 18 horas.

Tratamiento de eventos de prioridad "Alta": ante la ocurrencia de un evento de esta naturaleza, el CONTRATISTA se compromete a brindar un diagnóstico y vías de solución al problema en un plazo no superior a las 24hs laborales de haber recibido la comunicación correspondiente por parte de la UE003.

Tratamiento de eventos de prioridad "Normal": El CONTRATISTA acordará con la UE003 el plazo de solución a estos eventos en forma puntual, el cual no podrá extenderse por más de una semana. La UE003 indicará el momento más oportuno para la intervención correspondiente.

Tratamiento de eventos de prioridad "Baja": El CONTRATISTA acordará con la UE003 el plazo de solución a estos eventos en forma puntual, priorizando su resolución según backlog de incidentes. La UE003 indicará el momento más oportuno para la intervención correspondiente.

- **Incidente**: Se define como la interrupción no planificada o reducción de la calidad en los servicios base que fueron habilitados en la Plataforma de Nube Pública para soportar el sistema catastral. No se relaciona al funcionamiento del sistema.
  Un incidente también podrá ser originado como resultado de las alertas generadas por las herramientas de monitoreo y/o gestión de servicio de manera repentina.

- **Problema:** Se define como la causa desconocida de un incidente o múltiples incidentes con síntomas comunes, que afectan a los servicios habilitados en la Plataforma de Nube Pública. No se relaciona al funcionamiento del sistema.

Los niveles de servicio deben considerarse de acuerdo con los siguientes escenarios:

- La atención de incidentes y problemas en los ambientes de la plataforma de Nube Pública debe ser realizada durante horario 24x7x365. Son considerados servicios de soporte remoto y a demanda.

- El Proveedor debe considerar la cantidad de recursos necesarios para atender las incidencias y problemas las cuales pueden tener diversos tiempos de solución sobre la causa raíz de origen.

10. Metodología

El CONTRATISTA deberá recabar la información necesaria referente al cumplimiento de los requerimientos de los presentes Términos de Referencia.

- El CONTRATISTA deberá realizar el monitoreo de la Infraestructura de Servidores a proveer para asegurar los SLA de disponibilidad del servicio.
- El CONTRATISTA estará a cargo de las operaciones de respaldo y restauración de los servidores a proveer. Se coordinará en conjunto, con la Unidad Ejecutora 003, la frecuencia.
- El CONTRATISTA estará a cargo del soporte y gestión de la infraestructura base hasta los Sistemas Operativos a proveer.
- La Unidad Ejecutora 003 será responsable de gestionar y brindar soporte a las aplicaciones y servicios montados sobre la infraestructura de servidores.

11. Entregables

11.1 Primer Entregable

Habilitación de los servicios de Cloud Computing y creación de la cuenta de servicio. Acta de instalación y configuración de la infraestructura requerida. Plazo hasta 30 días.

11.2 Entregable Mensual

Informe conteniendo lo especificado en el alcance del servicio. Será presentado mensualmente, reportando los consumos, incidentes, estadísticas, estado actual, interacciones, soporte y otros indicadores de gestión.

12. CONDICIONES DEL SERVICIO

12.1 Plazo de Ejecución

EL CONTRATISTA se obliga a brindar el Servicio de Cloud Computing solicitado por un plazo mínimo de 12 meses o hasta culminada la bolsa contratada, los cuales podrán ser renovados, de acuerdo con la evaluación del servicio y la necesidad del Proyecto para el cumplimiento de sus objetivos. Este plazo se inicia a partir del día siguiente de la suscripción del Acta de instalación y configuración de la infraestructura requerida.

12.2 Plazo de Ejecución

- El CONTRATISTA deberá contar con un sistema de mesa de ayuda para atender los incidentes y requerimientos reportados por la Unidad Ejecutora 003.
- El tipo de contacto será el portal Web designado para dicho fin.
- Se asignará un número de ticket para seguimiento.
- El servicio de soporte local estará disponible 24x7
- Se deberá considerar un plan de soporte de una bolsa de 5 horas al mes:
  - Se trazará un plan de soporte entre el equipo de la UE003 y el CONTRATISTA.
  - Para los casos en que el tiempo de dedicación pueda ser estimada, el CONTRATISTA avisará al personal de la UE003 en el caso de que un incidente lleve más de las horas mensuales estipuladas.
- Las siguientes son consideraciones que aplican al esquema de soporte mensual con el CONTRATISTA:
  - El CONTRATISTA velará por la optimización de las horas de soporte, principalmente, para los incidentes asociados a consultas y capacitación con el objetivo de maximizar la productividad de la bolsa contratada.
  - El plan de soporte propuesto es para atención en días laborables de Perú, en el horario de 9:00hs a 18:00hs. En caso de requerir soporte en horario extendido o 24x7 se podrá coordinar con el CONTRATISTA.
  - El plan de soporte debe ser ejecutado por un mínimo de 12 meses.

12.3 Transferencia de Conocimiento / Capacitación

- El CONTRATISTA deberá realizar un taller de trabajo dirigido al personal de Sistemas de la Unidad Ejecutora 003, responsables y/o coordinadores del presente servicio a contratar (5 personas).
- EL CONTRATISTA deberá realizar una transferencia de conocimiento sobre la arquitectura de la solución, la infraestructura tecnológica a utilizar y sobre los procedimientos realizados para la gestión de la infraestructura.
- EL CONTRATISTA deberá también hacer de conocimiento con el personal de la Unidad Ejecutora 003 los procedimientos para la gestión de incidentes y requerimientos que son propios del proveedor de nube pública.
- La transferencia de conocimiento será de un mínimo de 4 sesiones de 2 horas cada sesión.

13. CARACTERÍSTICAS DEL POSTOR

a) EL POSTOR que desee participar en el presente proceso de contratación, debe ser una empresa jurídica debidamente constituida, que no esté comprendida en el Registro de Inhabilitados para contratar con el Estado, que se encuentre inscrita en el Registro Nacional de Proveedores capítulo de proveedores de servicios.
b) El proveedor del servicio en nube debe brindar el soporte técnico durante todo el tiempo que dure el servicio a contratar, es decir, durante un periodo de 365 días calendarios o hasta alcanzar el consumo de la bolsa de créditos, computados a partir de suscrita el acta de inicio del servicio
c) El proveedor debe contar con certificación otorgada por parte de la marca, que lo certifique como socio estratégico de nivel intermedio o superior o similares dicha certificación será presentada a través de una carta emitida por el fabricante, tomando como ejemplo lo siguiente

I. Nivel Avanzado o superior

d) El servicio de nube será brindado directamente por un proveedor de servicios en Nube que cuente con un socio comercial legalmente establecido en el Perú y cuente con la acreditación y certificación solicitada en el literal “c”, que este otorgue y que se encuentra facultado para comercializar sus servicios, como operarlos, gestionarlos y brindar soporte. Así mismo el socio comercial debe tener experiencia brindando servicios similares en otros países de Latinoamérica.
e) El POSTOR deberá brindar el servicio con la Infraestructura tecnológica como servicio (nube) de un fabricante de nube pública reconocido, al cual represente en el país. Para ello, deberá presentar una carta donde se indique que es el representante de la marca
f) EL POSTOR debe ser una empresa especializada en Servicios de Tecnologías de Información, debidamente organizada con capacidad y experiencia documentada para proporcionar los servicios solicitados.
g) El POSTOR deberá proponer en su oferta, los planes de ahorro y optimización de costos correspondientes a la reserva de recursos por el tiempo de contrato de 12 meses y deberá detallar las características de estos planes de ahorro, que tienda a que la facturación mensual se optimice.
h) El POSTOR deberá indicar, que se revisará el consumo mensual de los recursos, así como los planes de ahorro, para recomendar los ajustes necesarios que permitan optimizar el uso de los servicios Cloud.
i) El Monto Facturado por el POSTOR en servicios acumulados de Hosting Cloud de Aplicaciones o Servicios de Infraestructura en la nube pública, durante un periodo no mayor a cinco (05) años a la fecha de presentación de las propuestas, debe ser mayor o igual a S/ 800,000.00, lo cual se deberá acreditar con copia simple de los comprobantes de pago cancelados o, en su defecto del contrato y su respectiva conformidad de la prestación del servicio ejecutado por el Postor (no se aceptan declaraciones juradas). Estos servicios deben ser de clientes en Perú, en plataformas de nube y servicios asociados a la operación, administración soporte y gestión de este tipo de entornos.
j) No se tomará en cuenta la experiencia del POSTOR en Servicios de Hosting físico y/o virtual relacionados con el alojamiento de páginas Web, servicios VPS o Correo Electrónico.
k) El POSTOR al presentar su oferta, deberá revisar y cumplir obligatoriamente las especificaciones técnicas y/o exigencias que se detallan en las Bases Técnicas y demás documentos que conforman las Bases del Proceso de Contratación.
l) El POSTOR deberá de presentar en su propuesta, una estructura de costos en base a los ítems:

1. Costo único de implementación (levantamiento de requerimiento, diseño, implementación).
2. Costo mensual de administración o facturación local
3. Costo mensual de soporte (soporte después de implementado el servicio, cambios menores de configuración, respaldos, etc).
4. Cantidad ofertada de horas mensuales del plan de soporte.
5. Costo por hora adicional de soporte fuera del plan de soporte ofertado.
6. Costo por componente de infraestructura y por servicios.
7. Otros costos relacionados al servicio.

14. PERSONAL CLAVE

A. (1) Jefe de Proyecto

Formación académica:

Mínimo Título Profesional en Ingeniería de Sistemas y/o Ingeniería de Sistemas e Informática y/o Ingeniería Informática y de Sistemas y/o Ingeniería de Redes y Comunicaciones y/o Ingeniería Empresarial y/o Ingeniería en Computación y/o Ingeniería de Computación y Sistemas.

Experiencia:

Mínimo cinco (5) años de experiencia general en empresas públicas o privadas, de preferencia con consultorías en el ámbito internacional.
Experiencia gestionando equipos multidisciplinarios
Experiencia gestionando Proyectos de TI.
Experiencia gestionando Soluciones en Nube de la marca de la solución.

Capacitación:

Certificado como arquitecto profesional sobre la plataforma de la nube a ofertar.
Certificado como ingeniero DevOps profesional sobre la plataforma de la nube a ofertar.
Ambas certificaciones internacionales deben estar activas, se validará la certificación en la web de la nube ofertada.

Actividades:

- Realizará las coordinaciones con el personal de la Unidad Ejecutora 003. Además, informará sobre el avance de la implementación.
- Responsable del diseño e implementación de la arquitectura cloud.
- Realizará recomendaciones sobre la arquitectura o nuevas arquitecturas a desarrollarse.
- Realizará la actualización o mejoras a la arquitectura, de acuerdo a las necesidades de COFOPRI.

B. (01) Especialista Cloud

Formación académica:

Mínimo Título Profesional en Ingeniería de Sistemas e Informática, Ingeniería de Sistemas, Ingeniería en Computación, Ingeniería en Informática, Ingeniería de Sistemas Empresariales o Redes y Comunicaciones.

Experiencia:

Experiencia mínima de tres (3) años realizando implementación en Soluciones en Nube y/o Diseño de Servicios en Nube y/o implementación de arquitecturas de Nube.

Capacitación

Certificado como arquitecto profesional sobre la plataforma de la nube a ofertar.
Certificado como ingeniero DevOps profesional sobre la plataforma de la nube a ofertar.
Ambas certificaciones internacionales deben estar activas, se validará la certificación en la web de la nube ofertada.

Actividades:

- Administración de la infraestructura de COFOPRI
- Brindará soporte a los requerimientos de la Unidad Ejecutora 003.
- Elaborará las actas de reunión de trabajo e informará sobre el estado mensual del servicio y realizará la presentación del mismo

15. CONFIDENCIALIDAD

EL CONTRATISTA del servicio se compromete a mantener en reserva, y no revelar a tercero alguno, toda información a la que tenga acceso o que le sea suministrada por parte de la Unidad Ejecutora 003.

EL CONTRATISTA del servicio deberá adoptar bajo responsabilidad las medidas de índole técnica y organizativas necesarias para que el contenido de dicha información no se divulgue a terceros, para garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos suministrados y los riesgos a que están expuesto, ya provengan de la acción humana o del medio físico o natural, tomando las medidas necesarias.

16. PLAZO Y ENTREGABLES DEL SERVICIO

Plazo

EL CONTRATISTA se obliga a brindar el Servicio de Cloud Computing solicitado por un plazo mínimo de 365 días calendarios o hasta culminada la bolsa de créditos contratada, los cuales podrán ser renovados, de acuerdo con la evaluación del servicio y la necesidad del Proyecto para el cumplimiento de sus objetivos. Este plazo se inicia a partir del día siguiente de la suscripción del Acta/Constancia de instalación y configuración de la infraestructura requerida

Entregables

Un informe mensual del servicio brindado, el mismo que deberá contener como mínimo:

- Enumerar los servicios específicos utilizados durante el período. Esto debe incluir detalles sobre la capacidad de procesamiento, almacenamiento, bases de datos, servicios adicionales contratados.
- Proporcionar datos sobre el uso y métricas del servicio durante el período de facturación, como el tiempo de disponibilidad (expresado en porcentaje, tiempo de actividad en relación con el tiempo total), el consumo de recursos y cualquier información relevante para analizar la utilización de la Plataforma en la nube. Recomendaciones de escalabilidad de ser el caso.
- Reporte de Incidentes ocurridos, detalle del incidente, prioridad, tiempo de respuesta, tiempo de atención, tiempo sin servicio parcial o total recomendaciones de ser el caso.
- Reporte de requerimientos efectuados por la UE 003 durante el periodo, prioridad, tiempo de atención, tiempo de respuesta, recomendaciones.

17. PROPIEDAD INTELECTUAL

Todos los derechos tanto intelectuales como materiales y los que deriven sobre los contenidos, código fuente, formatos, documentos, productos, prototipos, etc. resultante de este servicio, serán propiedad exclusiva de la UE 003 de Cofopri, quien dispondrá de su libre difusión. Asimismo, TODOS los derechos tanto intelectuales como materiales y los que deriven sobre las grabaciones en videos del uso funcional de la solución informática, imágenes en movimiento, con o sin sonido, así como la explicación de la solución informática pasarán a ser propiedad de la UE 003 de Cofopri.

La UE 003 de Cofopri, tendrá la titularidad íntegra y exclusiva sobre los derechos de proporcionar a otras entidades, la solución informática producto del servicio, sin restricción en el ámbito nacional e internacional. En este sentido, la UE003 tendrá, entre otras prerrogativas reconocidas en el Perú por la Ley sobre el Derecho de Autor aprobada por el Decreto Legislativo Nº 822, el derecho exclusivo de

realizar, autorizar o prohibir el uso o distribución de la solución informática:
- Registrarlo ante Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (Indecopi)
- La reproducción por cualquier forma o procedimiento.
- La comunicación al público por cualquier medio.
- La traducción, adaptación, arreglo u otra transformación.

18. SISTEMA DE CONTRATACION Y FORMA DE PAGO

A. SISTEMA DE CONTRATACION

El sistema de contratación será a suma alzada.

B. FORMA DE PAGO

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, se realizarán pagos mensuales, según la cantidad de recursos contratados y consumidos de la bolsa, para lo cual, la Entidad debe contar con la siguiente documentación:

Primer Entregable (hasta 30 días de firmado el contrato)

Culminada la implementación y puesta en marcha del servicio.
- Acta de inicio de servicio que será firmado por la UE003
- Conformidad de implementación y puesta en marcha del servicio, emitido por la UE003, previa opinión técnica favorable del especialista de Sistemas y TI del proyecto.
- Pago del 5% del monto total

Entregable mensual. (Cada 30 días después de la puesta en marcha del servicio, durante doce (12) meses o hasta agotar la bolsa de servicio contratado)
Informe del servicio efectivamente prestado, con los montos facturados por el consumo de la bolsa contratada y soporte mensual.
Conformidad del servicio del entregable mensual, emitido por la Coordinación de Catastro de la UE003, previa opinión técnica favorable del especialista de Sistemas y TI del proyecto.

En caso de requerirse horas de soporte adicionales a los planes ofertados, estas deben ser cobradas en el siguiente mes de la facturación.

COFOPRI
Firmado digitalmente por BULEJE PUN Christian Enrico FAU 20306484479 soft
Motivo: Soy el autor del documento
Fecha: 09.11.2023 16:34:13 -05:00

COFOPRI
Firmado digitalmente por NEIRA REYMER Jose Antonio FAU 20306484479 soft
Motivo: Soy el autor del documento
Fecha: 09.11.2023 16:46:27 -05:00