

ESPECIFICACIONES TÉCNICAS

PLATAFORMA DE DESPLIEGUE DE LA ARQUITECTURA DESACOPLADA DE GESTION DEL REGISTRO UNICO DE PERSONAS (SIIRC) – PARA LOS AMBIENTES DE DESARROLLO, INTEGRACIÓN Y PRUEBAS

I. ANTECEDENTES:

El Registro Nacional de Identificación y Estado Civil (RENIEC) es un organismo público constitucionalmente autónomo que cuenta con personería jurídica de derecho público interno y goza de atribuciones exclusivas y excluyentes en materia registral, técnica, administrativa, económica y financiera.

Sus funciones principales son organizar y mantener actualizado el Registro Único de Identificación de las Personas Naturales (RUIPN) de manera permanente; dirigir y administrar el sistema registral que involucra el registro civil, el registro de personas y el registro de naturalización, que en conjunto permiten construir la base de datos de identificación de todos los peruanos.

En la época electoral, participa activamente como parte del sistema electoral, junto con el Jurado Nacional de Elecciones (JNE) y la Oficina Nacional de Procesos Electorales (ONPE).

En este contexto, para responder a la misión del RENIEC, la República del Perú y el Banco Interamericano de Desarrollo – BID suscribieron el 06 de febrero de 2019 el Contrato de Préstamo BID № 4297/OC-PE, con la finalidad que dicho organismo financie parcialmente el proyecto denominado “Mejoramiento del acceso a los servicios de Registros Civiles e Identificación de calidad a nivel nacional”, el mismo que se centrará en resolver los problemas concernientes al limitado acceso de la población a los servicios de “Registros Civiles e Identificación de Calidad”.

La ejecución del Proyecto se prevé aproximadamente en cuatro (4) años siendo su horizonte de beneficios alrededor de diez (10) años. Para ello, se estimó que el costo total del proyecto será de USD 80 millones, de los cuales el Banco Interamericano de Desarrollo BID - otorgará un financiamiento parcial que representa el 62.3% y como contraparte el RENIEC brindará el 37.7%.

El objetivo general del proyecto es lograr un adecuado acceso de la población a los servicios de registros civiles e identificación de calidad a nivel nacional, mediante la reducción del costo de transacción asignada a la población que busca obtener estos servicios. Por ende, para la consecución del objetivo se han establecido los siguientes componentes:

Componente 1: Adecuada cobertura de los servicios presenciales con el objetivo de mejorar la atención presencial en Agencias con el uso de tecnología.

Componente 2: Mayor prestación de servicios a población vulnerable con el objetivo de Mejorar la atención de servicios en comunidades lejanas.



Componente 3: Incorporación de tecnologías para la prestación de los servicios con el objetivo de Renovación de sus Sistemas Transaccionales.

Estos Componentes tienen tres objetivos: 1) Mejorar la atención presencial en Agencias con el uso de tecnología, 2) Mejorar la atención de servicios en comunidades lejanas y 3) Renovación de sus Sistemas Transaccionales.

II. CONTEXTO DEL PROYECTO DEL SIIRC

En el marco del Proyecto se plantea implementar sistemas de información gerencial, servidores de producción, desarrollo de aplicaciones de software y base de datos, así como el mejoramiento del PKI; los elementos mencionados permiten el soporte a las actas registrales y capturas en vivo; finalmente sensibilizar a la población en el uso adecuado de las nuevas tecnologías destinadas a los servicios de registro civil e identificación. En dicho contexto, se plantea la actividad “Sistema Integrado de Identificación y Registro Civil (SIIRC)” que forma parte del Producto 17: Sistema Integrado de Identificación y Registro Civil (SIIRC) implementado.

La actividad “Sistema Integrado de Identificación y Registro Civil (SIIRC)”, tiene como objetivo desarrollar un sistema informático único e integral que soporte tecnológicamente los procesos misionales del RENIEC en sus seis bloques de registros: Identificación, Registro Civil, Servicio Electoral, Registro de Certificación Digital y Servicios Digitales, Servicios de Información y Vínculo de Parentesco. Esta actividad se va a llevar a cabo considerando las siguientes etapas:

- Análisis y Diseño, tiene como alcance llevar a cabo la actualización de los procesos TO BE de la Arquitectura Institucional y la elaboración del análisis y diseño de los procesos misionales. Los procesos están agrupados de la siguiente manera: Identificación, Registro Civil, Servicio Electoral, Certificación Digital y Servicios Digitales, Servicios de Información, y Vínculo de Parentesco.
- Desarrollo de Software, tiene como alcance llevar a cabo el desarrollo del sistema SIIRC basado en la arquitectura desacoplada y CI/CD (Continuous Integration - Integración continua / Continuous Deployment - Entrega o implementación continua).
- Migración de datos, tiene como alcance llevar a cabo la migración de la data histórica de los procesos misionales mediante el uso de herramientas ETL, desde las plataformas actuales hacia el nuevo repositorio de información.
- Plataforma de despliegue, tiene como alcance la adquisición, instalación y configuración de la plataforma de hardware y software como nube privada (on-premise), herramientas de DevSecOps y las herramientas de software para cada una de las capas de la arquitectura desacoplada para los ambientes de desarrollo, integración, pruebas y producción, adicionalmente el soporte y mantenimiento. Esta etapa está conformada por las siguientes fases:
 - Fase 1: Plataforma de despliegue para los ambientes de desarrollo, integración y pruebas (**lo cual es el objetivo del presente documento**).
 - Fase 2: Plataforma de despliegue para el ambiente de producción.



- Despliegue e implantación, tiene como alcance la comunicación, adaptación de los puestos de trabajo, gestión del cambio, capacitación operacional y acompañamiento; con la finalidad de minimizar el impacto y preparar a la organización para la puesta en marcha del nuevo sistema SIIRC.

En este contexto, el RENIEC ejecutó una primera fase del proyecto que fue la elaboración de su Arquitectura Institucional, basado en una nueva estrategia y visión al 2030 y sus correspondientes nuevos modelos: de negocio (estrategia y procesos) y de tecnología (datos, aplicaciones e infraestructura). El resultado de esta primera fase del proyecto ("Elaboración de la Arquitectura Institucional Enfocada en Procesos del RENIEC") es uno de los insumos para la implementación del Sistema Integrado de Identificación y Registro Civil que soportará el nuevo modelo de registros de personas del RENIEC.

III. OBJETIVO DE LA CONTRATACIÓN:

Contar con una plataforma de gestión de contenedores para los ambientes de desarrollo, integración y pruebas del Sistema Integrado de Identificación y Registro Civil (SIIRC), para la etapa de Desarrollo de Software.

OBJETIVO GENERAL

El objetivo es la adquisición, instalación y configuración de la plataforma de hardware y software como nube privada (on-premise) y de las herramientas de software para las capas de la arquitectura desacoplada para los ambientes de desarrollo, integración y pruebas del Sistema Integrado de Identificación y Registro Civil (SIIRC), considerando como paso previo a la ejecución de la etapa Desarrollo de Software.

Esta plataforma será destinada para que el contratista de la fase de Desarrollo de Software haga uso de estas con las herramientas definidas en el presente proceso, tomando en consideración los estándares aprobados por la oficina de tecnología e información de RENIEC.

OBJETIVOS ESPECÍFICOS

Instalación y configuración de la infraestructura

Implementar la plataforma de orquestación de contenedores en una infraestructura de nube privada (on premise), asegurando que todos los componentes necesarios estén correctamente instalados y configurados.

Configurar la infraestructura de hardware adecuada, incluyendo servidores, almacenamiento y redes, para soportar eficientemente la plataforma de orquestación de contenedores.

Garantizar Alta Disponibilidad y Escalabilidad

Configurar la plataforma de orquestación de contenedores para garantizar alta disponibilidad (HA) y escalabilidad horizontal, asegurando que la plataforma pueda manejar incrementos en la carga de trabajo sin interrupciones.



Monitorear el Desempeño de la Plataforma

Implementar una solución de monitoreo que permita supervisar el desempeño de la plataforma de orquestación de contenedores en tiempo real.

Conformidad con los estándares de RENIEC

La plataforma de orquestación de contenedores y las herramientas integradas deberán cumplir con los estándares técnicos y de seguridad aprobados por la Oficina de Tecnologías de la Información del RENIEC.

Asegurar la interoperabilidad de la plataforma de orquestación de contenedores con los sistemas existentes y futuros del RENIEC.

Integrar Herramientas de Desarrollo y DevSecOps

Proveer e integrar las herramientas de desarrollo de software y DevSecOps con la plataforma de orquestación de contenedores, la cual debe comprender como mínimo las siguientes herramientas:

1. Gestor de Código Fuente (herramienta que permite versionar el código fuente de las aplicaciones que se vayan desarrollando).
2. Registro de Contenedores (herramienta esencial para almacenar, organizar y compartir imágenes de contenedores de software).
3. Repositorio de Artefactos (herramienta que permite almacenar, organizar y gestionar de manera centralizada los artefactos de software, como librerías, archivos binarios, y paquetes que se generan durante el desarrollo).
4. Gestor de automatización de la construcción del software, pipelines de integración y entrega continua (CI/CD) (herramienta que automatiza el proceso de desarrollo y despliegue de software, asegurando que los cambios se integren y entreguen de manera rápida y sin errores).
5. Gestor de Pruebas de Performance (herramienta que evalúa el rendimiento de una aplicación bajo diversas condiciones para asegurar que funcione de manera eficiente y estable).
6. Análisis estático de código fuente (herramienta que analiza el código fuente de una aplicación para detectar vulnerabilidades de seguridad antes de que el software se ejecute).
7. Escaneo de vulnerabilidades en contenedores (herramienta que detecta posibles fallos de seguridad en las imágenes de contenedores antes de que se utilicen en producción).
8. Automatización de Operaciones de TI (herramienta que automatiza actividades complementarias al proceso de desarrollo y despliegue de software para los sistemas legados que se integren con la plataforma de contenedores).

Configurar las herramientas para los ambientes de desarrollo, integración y pruebas para que estén listas para su uso en la etapa de Desarrollo del Software.

Se requiere que el contratista provea licencias perpetuas o suscripciones de las herramientas de desarrollo y DevSecOps. La modalidad de licenciamiento o



suscripción requerida en la presente contratación será definida por cada herramienta en el Anexo 03.

Instalación y configuración de herramientas de la arquitectura desacoplada y base de datos

Implementar las herramientas de la arquitectura desacoplada sobre la plataforma de orquestación de contenedores, la cual debe comprender las siguientes herramientas:

- Software de API Manager
- Software de Autenticación para la Gestión de Identidades y Control de Accesos
- Software de Streaming de Datos en Tiempo Real
- Base de datos ORACLE

Configurar las herramientas para los ambientes de desarrollo, integración y pruebas para que estén listas para su uso en la etapa de Desarrollo de Software.

Se requiere que el contratista provea licencias perpetuas o suscripciones de las herramientas de la arquitectura desacoplada para los entornos de desarrollo, integración y pruebas. La modalidad de licenciamiento o suscripción requerida en la presente contratación será definida por cada herramienta en el Anexo 04.

Proveer Documentación y Transferencia de Conocimiento

Elaborar el plan de transferencia de conocimiento y documentación detallada sobre la plataforma de orquestación de contenedores, las herramientas integradas y la base de datos; asegurando que el personal del RENIEC pueda administrar, operar y mantener la plataforma teniendo en cuenta la continuidad, disponibilidad y seguridad.

Entregar las guías de usuario y manuales técnicos que faciliten la gestión diaria y la resolución de problemas.

IV. ALCANCE

Para la siguiente adquisición el contratista o proveedor adjudicado debe cumplir con el siguiente alcance como mínimo:

- Adquirir e instalar los servidores, el almacenamiento y la infraestructura de red necesarios para soportar la plataforma de orquestación de contenedores. Las especificaciones técnicas se encuentran en el Anexo 01.
- Preparar el ambiente de instalación en el centro de datos proporcionado por el RENIEC, asegurando que cumpla con los requisitos de hardware y software especificados.



- Instalar y configurar los componentes de la plataforma, incluyendo el motor de orquestación, el registro de contenedores y el panel de control. Las especificaciones técnicas se encuentran en el Anexo 02.
- Configurar los servidores, el almacenamiento y la red de la infraestructura según las mejores prácticas para garantizar un rendimiento óptimo y una alta disponibilidad.
- Establecer políticas de seguridad y acceso provistas por la plataforma de orquestación de contenedores para proteger los datos y recursos.
- Implementar estrategias de redundancia y failover provistas por la plataforma de orquestación de contenedores para garantizar la disponibilidad continua de los servicios ofrecidos.
- Configurar la capacidad de escalabilidad automática para que la plataforma de orquestación de contenedores pueda adaptarse dinámicamente a las variaciones en la carga de trabajo.
- Implementar y configurar una herramienta de monitoreo para supervisar el desempeño de la plataforma de orquestación de contenedores en tiempo real.
- Configurar la capacidad de escaneo de vulnerabilidades para que la plataforma de orquestación de contenedores pueda detectar vulnerabilidades a nivel de contenedores.
- Configurar los ambientes de desarrollo, integración y pruebas para la implementación del SIIRC, cuyas características son:
 - Ambiente de desarrollo, es el entorno destinado para la integración de los desarrollos.
 - Ambiente de integración, es el entorno destinado para las versiones preliminares.
 - Ambiente de pruebas, es el entorno destinado para las versiones beta.
- Instalar y configurar las herramientas de desarrollo de software y DevSecOps con la plataforma de orquestación de contenedores para los ambientes de desarrollo, integración y pruebas. Las especificaciones técnicas se encuentran en el Anexo 03.
- Instalar y configurar las herramientas de la arquitectura desacoplada sobre la plataforma de orquestación de contenedores para los ambientes de desarrollo, integración y pruebas. Las especificaciones técnicas se encuentran en el Anexo 04.
- Realizar pruebas de cumplimiento para verificar que la plataforma y sus componentes cumplan con estándares técnicos y de seguridad.



- Documentar los resultados de las pruebas de cumplimiento y tomar medidas correctivas según sea necesario.
- Elaborar la documentación detallada que describa la configuración inicial de la plataforma y los procedimientos de operación.
- Elaborar la documentación de la arquitectura implementada y de la configuración de las bases de datos configuradas.
- Elaborar la documentación de administración de encendido y apagado de la plataforma de base de datos Oracle.

V. ACTIVIDADES O TAREAS MINIMAS A REALIZAR:

Para la siguiente adquisición el contratista o proveedor adjudicado debe cumplir con las siguientes actividades como mínimo:

1. PLAN DE TRABAJO:

- Elaborar el plan de trabajo, que comprende la adquisición, instalación y configuración de la plataforma de orquestación de contenedores, de las herramientas de desarrollo (DEVSECOPS), las herramientas de software para las capas de la arquitectura desacoplada, y la base de datos ORACLE. El plan de trabajo debe ser validado y aprobado por la Unidad de Infraestructura y Soporte Tecnológico (UIST) de la Oficina de Tecnologías de la Información (OTI). El cronograma de actividades debe contener:
 - Personal
 - Organización
 - Estrategia
 - Recursos
- Realizar una presentación de la metodología, personal del contratista y el plan de trabajo al Equipo Técnico de Trabajo (ETT), con el fin de involucrarlos en el desarrollo de las actividades.
- Realizar reuniones de coordinación con el Equipo Técnico de Trabajo (ETT), para revisar los avances del trabajo y asegurar el cumplimiento de las actividades. La primera reunión presencial se realizará en el transcurso de los cinco días hábiles siguientes de la firma del contrato. Las reuniones podrán ser realizadas de manera virtual, y de manera presencial al menos una reunión cada 30 días calendario.
- Las actividades mínimas que deberá realizar el Jefe de Proyecto son las siguientes:
 - Desarrollo del plan de trabajo.
 - Planear y seguimiento de las actividades de implementación y mantenimiento.



- Seguimiento de la atención de soporte in situ y/o remoto.
- Cierre del proyecto.

- Las actividades mínimas que deberá realizar el Arquitecto de la Solución son las siguientes:

- Análisis de la infraestructura tecnológica.
- Diseño y gestión de la arquitectura basado en microservicios.
- Implementación de la plataforma de microservicios en los ambientes de desarrollo, integración y pruebas.
- Implementación de las herramientas que conforman la arquitectura desacoplada.
- Recomendaciones de mejores prácticas para la gestión de servicios de soporte.

- Las actividades mínimas que deberá realizar el Especialista de Plataforma de Orquestación de Contenedores son las siguientes:

- Propuesta para la configuración de la plataforma de gestión de contenedores.
- Propuesta para la actualización y habilitación de los componentes utilizados en la plataforma de contenedores.
- Mejora y resolución de incidentes en el ambiente de desarrollo, integración y pruebas según reporte la entidad.
- Propuesta de mejora de performance de la plataforma de contenedores.
- Revisión y monitoreo de todos los componentes de la plataforma de contenedores.

- Las actividades mínimas que deberá realizar el Especialista de DevSecOps son las siguientes:

- Propuesta para la configuración de las herramientas para el flujo DevSecOps.
- Implementación y configuración de las herramientas del flujo de DevSecOps.
- Implementación y despliegue de un microservicio en el flujo DevSecOps que interactúe con los ambientes de desarrollo, integración y pruebas.
- Recomendaciones de mejores prácticas para la gestión de las herramientas.

- Las actividades mínimas que deberá realizar el Administrador de Base de Datos ORACLE son las siguientes:

- Análisis de la infraestructura tecnológica.
- Instalar y configurar el Software de Oracle Database Enterprise Edition.
- Revisión y monitoreo de todos los componentes de la base de datos.
- Recomendaciones de mejores prácticas para la gestión de servicios de soporte.



2. ADQUISICIÓN, INSTALACIÓN Y CONFIGURACIÓN:

- Adquirir, instalar y configurar los servidores, el almacenamiento y la infraestructura de red necesarios para soportar la plataforma de orquestación de contenedores.
- Preparar los ambientes de instalación en el centro de datos proporcionado por el RENIEC, asegurando que cumpla con los requisitos de hardware y software especificados.
- Instalar y configurar los componentes principales de la plataforma, incluyendo el motor de orquestación, el registro de contenedores y el panel de control.
- Configurar los servidores, el almacenamiento y la red de la infraestructura según las mejores prácticas para garantizar un rendimiento óptimo y una alta disponibilidad.
- Establecer políticas de seguridad y acceso provistas por la plataforma de orquestación de contenedores para proteger sus datos y recursos.
- Implementar estrategias de redundancia y failover provistas por la plataforma de orquestación de contenedores para garantizar la disponibilidad continua de los servicios ofrecidos.
- Configurar la capacidad de escalabilidad automática para que la plataforma de orquestación de contenedores pueda adaptarse dinámicamente a las variaciones en la carga de trabajo.
- Implementar y configurar una herramienta de monitoreo para supervisar el desempeño de la plataforma de orquestación de contenedores en tiempo real.
- Configurar la capacidad de escaneo de vulnerabilidades para que la plataforma de orquestación de contenedores pueda detectar vulnerabilidades a nivel de contenedores.
- Configurar los ambientes de desarrollo, integración y pruebas para la implementación del SIIRC.
- Instalar y configurar herramientas de desarrollo de software y DevSecOps con la plataforma de orquestación de contenedores.
- Instalar y configurar las herramientas de la arquitectura desacoplada con la plataforma de orquestación de contenedores.
- Realizar pruebas de cumplimiento para verificar que la plataforma y sus componentes cumplan con estándares técnicos y de seguridad.



- Elaborar la documentación de la arquitectura implementada y de la configuración de las bases de datos configuradas.
- Elaborar la documentación de administración de encendido y apagado de la plataforma de base de datos Oracle.
- Documentar los resultados de las pruebas de cumplimiento y tomar medidas correctivas según sea necesario.

3. IMPLEMENTACION Y DESPLIEGUE DEL FLUJO DEVSECOPS:

- La implementación y despliegue un flujo DevSecOps que utilice las herramientas de desarrollo y DevSecOps ofertadas, las cuales buscan garantizar la seguridad, calidad y agilidad en el ciclo de vida del desarrollo y operación de software.
- La implementación y despliegue del flujo DevSecOps deberá cubrir un (01) microservicio propuesto por el contratista, el cual deberá ser utilizado como prototipo para comprobar que el flujo de DevSecOps configurado se cumpla en todas sus etapas y entregue el resultado esperado. Este microservicio propuesto deberá ser desarrollado con la tecnología Java y que interactúe con los ambientes de desarrollo, integración y pruebas. Esta Implementación incorpora varias dimensiones clave:

Desarrollo Seguro (Dev):

Análisis Estático de Seguridad de Aplicaciones (SAST): Implementación de la práctica SAST mediante el análisis estático del código fuente del microservicio desarrollado en busca de vulnerabilidades de seguridad durante el desarrollo.

Integración Continua (CI):

Implementación de un (01) pipeline de CI que automatiza la construcción, prueba unitaria, análisis estático del código, versionamiento de empaquetado (jar, war o ear) del microservicio, construcción del contenedor que contiene el microservicio y escaneo de vulnerabilidades de seguridad en el contenedor, en cada cambio de código, asegurando la detección temprana de problemas.

Despliegue Seguro (Sec):

Gestión de Configuración Segura: Implementación de herramientas de gestión de configuración segura para asegurar que la infraestructura y las aplicaciones se mantengan consistentes y seguras en todos los entornos.

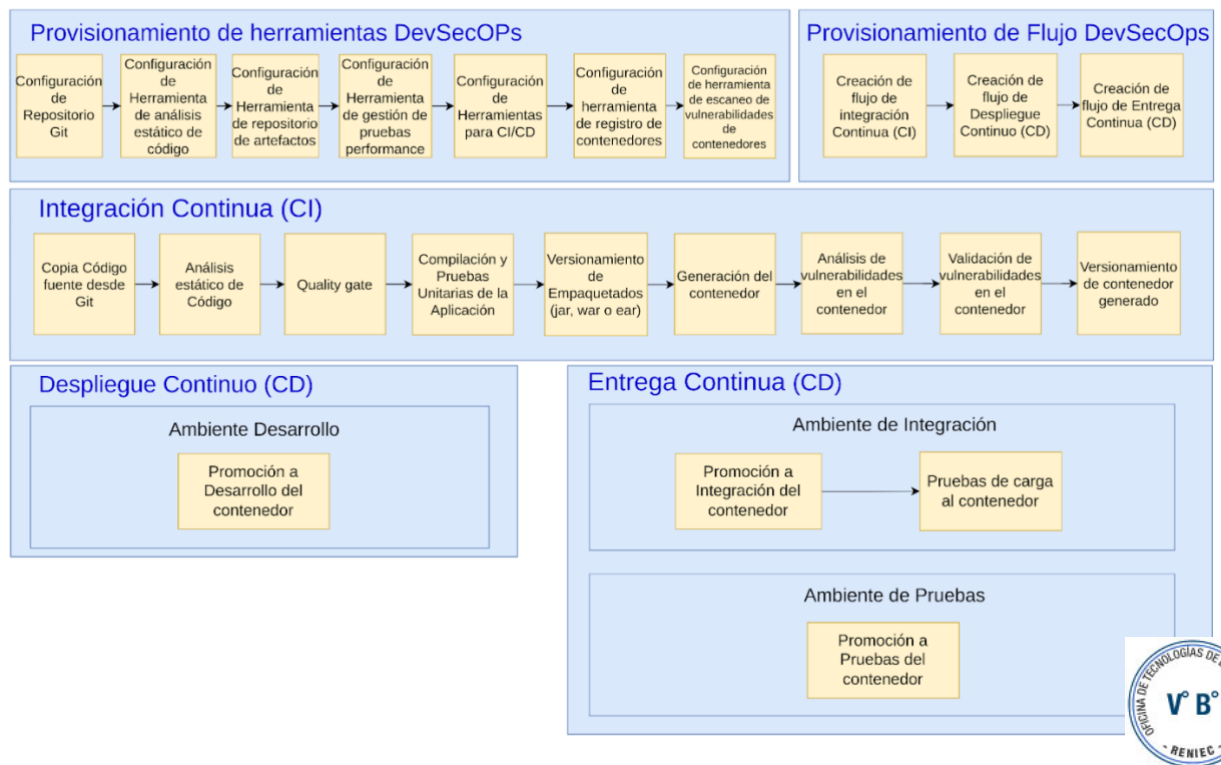
Pruebas de carga del microservicio (Performance Testing): Integración de la herramienta de gestión de pruebas de performance para un (01) microservicio.

Operación Segura (Ops):

Entrega Continua (CD): Establecimiento de dos (02) pipelines de CD que automatizan la entrega y despliegue de aplicaciones en entornos de integración y pruebas, con la ejecución de pruebas de performance del microservicio en el ambiente de integración.



A continuación, se detalla la cantidad mínima de actividades incluidas como parte de la implementación del flujo DevSecOps.



Provisionamiento de herramientas DevSecOps

Configuración de herramientas DevSecOps: Esta actividad tendrá como objetivo el realizar la instalación y configuración automatizada de las herramientas que formarán parte del proceso de DevSecOps que forma parte del flujo DevSecOps propuesto para un (01) microservicio.

Provisionamiento de flujo DevSecOps para un (01) microservicio

Creación del flujo DevSecOps: Consiste en configurar de forma automática los flujos para integración Continua (CI), Despliegue Continuo (CD) y Entrega Continua (CD) para un (01) microservicio.

Integración Continua (CI)

Copia Código fuente desde Git: Se debe iniciar el flujo de integración continua desde el momento en que se realiza un cambio en el repositorio de código fuente.

Análisis estático de Código: Para el microservicio se deberá realizar el análisis estático del código fuente.

Quality gate: Luego de realizar el análisis estático de código fuente, se valida si el umbral de calidad previamente configurado permite dar conformidad al código fuente analizado.



Compilación y pruebas unitarias del microservicio: Se realizará la compilación y ejecución de pruebas unitarias del microservicio a fin de tener un primer control de calidad de la aplicación.

Versionamiento de empaquetados: En caso de que el compilado y pruebas sean conformes, se generará un artefacto (war, jar o ear) el cual deberá ser versionado en la herramienta de repositorio de artefactos.

Generación del contenedor: Se procederá con la generación del contenedor utilizando el artefacto previamente generado y versionado.

Análisis de vulnerabilidades del contenedor: En caso de que la generación del contenedor sea conforme, se iniciará el análisis de vulnerabilidades del contenedor utilizando la herramienta de escaneo de vulnerabilidades del contenedor.

Validación de vulnerabilidades en el contenedor: Luego de realizar el análisis de vulnerabilidades del contenedor, se valida si el umbral de seguridad previamente configurado en la herramienta de escaneo de vulnerabilidades del contenedor permite dar conformidad al contenedor analizado.

Versionamiento del contenedor generado: Cuando las actividades anteriores son conformes, se genera un contenedor el cual deberá ser versionado en la herramienta de registro de contenedores.

Despliegue Continuo a Desarrollo (CD)

Promoción a Desarrollo del contenedor: Esta actividad automatiza el despliegue en plataforma de orquestación de contenedores para el ambiente de desarrollo. Para iniciar esta tarea no requiere de ningún tipo de aprobación y/o intervención humana.

Entrega Continua (Integración y Pruebas)

Promoción a integración del contenedor: Esta actividad automatiza el despliegue en plataforma de orquestación de contenedores para el ambiente de integración. Para iniciar esta tarea se requiere de una intervención humana.

Pruebas de carga al contenedor: Esta actividad debe integrar la ejecución de pruebas de performance usando la herramienta gestión de pruebas de performance ofertada.

Promoción a pruebas del contenedor: Esta actividad automatiza el despliegue en plataforma de orquestación de contenedores para el ambiente de pruebas. Para iniciar esta tarea se requiere de una intervención humana.

- La implementación y despliegue del flujo DevSecOps deberá cubrir un (01) microservicio de ejemplo que será provisto por el contratista. Es decir, deberá implementar la integración y automatización de operaciones de TI desde el provisionamiento de las herramientas hasta la puesta en pruebas del microservicio.



- Este flujo modelo DevSecOps busca ser una prueba de la integración de las herramientas DevSecOps ofertadas usando un (01) microservicio ejemplo que será provisto por el contratista. Cabe señalar que este flujo no representa la implementación final del proceso DevSecOps que implementará la institución posteriormente y la cual abarcaría más aplicaciones y/o microservicios.

4. TRANSFERENCIA DE CONOCIMIENTO:

- Elaborar el Plan de transferencia de conocimiento que debe contener al menos el siguiente detalle:
 - Tiempo de duración por cada acción de la capacitación
 - Horarios y cronograma de la ejecución
 - Modalidad remota
- Considerar las guías de usuario y manuales técnicos, los cuales serán dictados en español. El material podrá estar en idioma inglés.
- Brindar la transferencia de conocimientos, la cual debe cubrir los temas con la cantidad de horas lectivas (mínimo) y cantidad de participantes detallados a continuación:

Tema	Cantidad de Horas Lectivas	Cantidad de Participantes
Plataforma de orquestación de contenedores y las herramientas integradas	40	5
Base de datos	20	8

(*) La transferencia de conocimiento será realizada de manera virtual. Los horarios deben ser coordinados y aprobados con RENIEC.

VI. METODOLOGIA:

El contratista o proveedor adjudicado deberá tener en cuenta:

a. Plataforma de Orquestación de Contenedores

Las especificaciones de la Plataforma de Orquestación de Contenedores se encuentran en el Anexo 02.

b. Instalación, configuración e implementación de la plataforma de orquestación de contenedores, herramientas de la arquitectura desacoplada, herramientas de desarrollo, DevSecOps y base de datos Oracle.

El contratista deberá elaborar un plan de trabajo al inicio de las actividades de instalación, configuración e implementación de la plataforma de orquestación de



contenedores herramientas de la arquitectura desacoplada, herramientas de desarrollo, DevSecOps y base de datos Oracle.

Este plan de trabajo debe ser evaluado por la UIST/OTI, para su aprobación.

El contratista es responsable de la instalación, configuración e interconexión de los componentes de hardware, así como los componentes necesarios para el correcto funcionamiento de la plataforma de orquestación de contenedores, herramientas de la arquitectura desacoplada, herramientas de desarrollo, DevSecOps y base de datos Oracle. El RENIEC brindara el espacio para la puesta en marcha.

El contratista es responsable de la instalación y configuración de todo el licenciamiento o suscripciones y sus componentes necesarios para el correcto funcionamiento de la plataforma de orquestación de contenedores, herramientas de la arquitectura desacoplada, herramientas de desarrollo, DevSecOps y base de datos Oracle. RENIEC brindara facilidades de acceso para la instalación y puesta en marcha de la plataforma.

La implementación de las licencias o suscripciones de la plataforma de orquestación de contenedores debe considerar aspectos de gestión de contenedores, orquestación de contenedores, Api Server Scheduler, Controller Manager, seguridad, monitoreo de contenedores, a fin de que sirva de plataforma base para desplegar microservicios.

El contratista realizara la instalación y configuración de tres (03) ambientes, uno para desarrollo, otro para integración y otro para pruebas, sobre la infraestructura (hardware) propuesto en modalidad ON PREMISE. El contratista brindara la infraestructura que requiera para instalar la plataforma de orquestación de contenedores, debiendo el proveedor tomar en cuenta como mínimo el dimensionamiento de hardware mencionado en el Anexo 01.

El contratista deberá realizar la configuración de 03 ambientes, con la finalidad de que las cargas de trabajo sean independientes entre los ambientes.

El contratista deberá incluir todos los componentes de licenciamiento o suscripciones necesarios para que la herramienta de gestión de orquestación contenedores pueda ser implementada, para lo cual debe considerar lo especificado en los Anexos.

La instalación y configuración se podrá realizar de forma remota y estará a cargo del personal clave propuesto para el servicio, y de requerirse un personal que este en la sede de RENIEC para alguna actividad específica, este personal presencial podrá ser propuesto por el contratista.

El contratista deberá contar con una Mesa de Servicio o Mesa de Ayuda o Helpdesk o Plan de Asistencia Permanente, para el proceso de registro, soporte, solución de incidentes y problemas informáticos reportados por el RENIEC, para lo cual el contratista deberá presentar junto con su propuesta técnica una declaración jurada correspondiente.

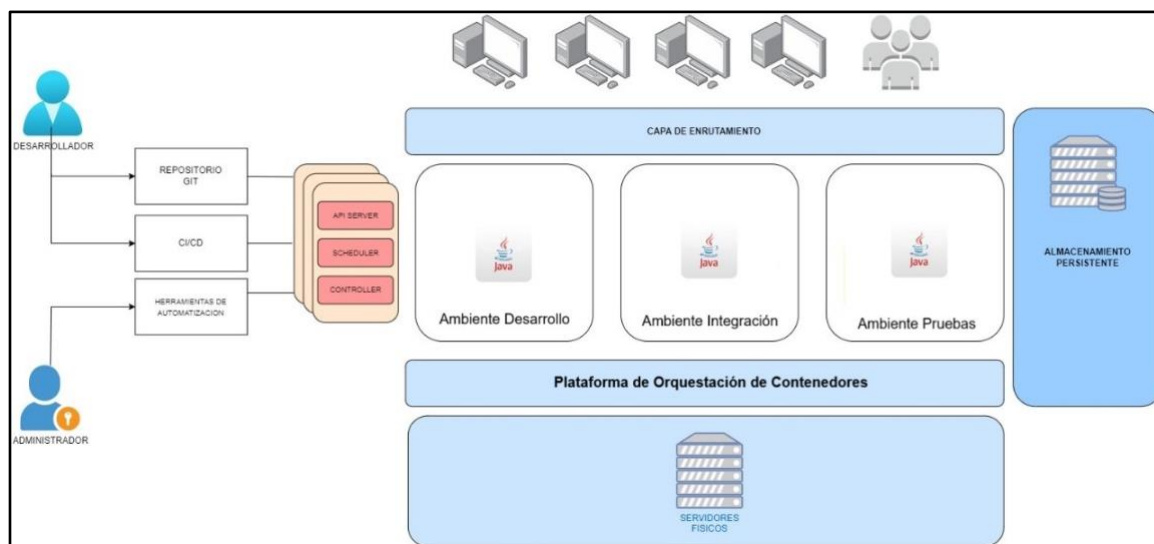
El contratista presentará una carta del fabricante que garantice la vigencia tecnológica de los equipos ofertados por 03 años, en la que se compromete a brindar el soporte de hardware; debiendo presentar este documento junto con su propuesta técnica.

El equipamiento ofertado debe incluir la Garantía del fabricante y/o subsidiaria, mínimo de 03 años, en la modalidad de 24x7x365, cubriendo repuestos, mano de obra y servicio On-Site. Para lo cual el contratista deberá presentar una carta



remitido por el fabricante en donde se precise el periodo de garantía y los datos básicos de los equipos. Este documento debe entregarse junto a los equipos, debiendo iniciar su vigencia desde la fecha de entrega de los equipos.

La Plataforma de Orquestación de Contenedores como referencia debe considerar:



c. Soporte Técnico

El contratista debe proporcionar el soporte del fabricante, que incluya el soporte y mantenimiento de versiones y actualizaciones del software de orquestación de contenedores ofertado, herramientas de la arquitectura desacoplada ofertada, herramientas de desarrollo, devsecops ofertada y base de datos Oracle a través de llamadas telefónicas, vía email o mediante la página web del fabricante durante el plazo de 03 años, contabilizados a partir del día siguiente de la entrega de las licencias o suscripciones.

Acceso ilimitado a los diferentes recursos técnicos del fabricante del software orquestador de contenedores ofertado, durante el periodo de 03 años.

Actualizaciones y parches (fixes) que puedan “liberarse” durante el periodo de vigencia del contrato sin costo alguno para el RENIEC.

Derecho a usar todas las actualizaciones que ponga a disposición el fabricante del software orquestador de contenedores ofertado, herramientas de la arquitectura desacoplada ofertada, herramientas de desarrollo, devsecops ofertada y base de datos Oracle que se encuentren liberadas por los respectivos fabricantes al inicio de la operación de la plataforma propuesta.

Realizar la atención de requerimiento de soporte técnico de la plataforma de orquestación de contenedores ofertada para:

- Consultas técnicas
- Realizar configuraciones y/o afinación de componentes

- Despliegue de microservicios

El servicio de soporte ante incidencias proporcionado por el contratista deberá incluir: análisis, determinación solución y documentación de incidentes suscitados a la plataforma de orquestación de contenedores ofertada.

El RENIEC efectuara llamadas de servicio de soporte para atención de incidentes y/o requerimiento al número telefónico proporcionado por el contratista. Las comunicaciones de solicitud de soporte podrán efectuarse telefónicamente o por correo electrónico.

El siguiente cuadro tiene la modalidad y tiempos máximos de atención esperados para soporte del contratista, ante incidencia y/o requerimientos:

INCIDENTES			
	NO CRITICO	CRITICO	REQUERIMIENTOS
Modalidad	8X5	24X7	8X5
Tiempo máximo de inicio de atención	(02) horas posteriores a la solicitud de soporte o según lo coordinado con el personal supervisor del servicio del RENIEC	(02) horas posteriores a la solicitud de soporte	(02) horas posteriores a la solicitud del requerimiento o según lo coordinado con el personal supervisor del servicio del RENIEC
Tiempo de resolución / Ejecución	(12) doce horas posteriores al inicio de la atención	(04) cuatro horas posteriores al inicio de la atención	(24) veinticuatro horas posteriores al inicio de la atención

Durante el periodo del contrato, el contratista deberá brindar:

- Un máximo de doscientos (200) atenciones anuales de soporte técnico para incidentes.
- Un máximo de cien (100) horas anuales para atender requerimientos.

Las atenciones de incidentes y/o requerimientos se realizarán de forma remota.

El proveedor deberá emitir un informe sobre los pedidos atendidos, indicando lo siguiente:

- Fecha y Hora de Solicitud
- Fecha y hora del Ticket
- Fecha y hora de Atención
- Fecha y hora de Cierre



- Quien lo reporta
- Medio
- Numero de Ticket
- Responsable
- Horas Ejecutadas
- Estado

d. Mantenimientos Programados

El contratista deberá realizar tres (03) servicios de mantenimientos programados y diagnostico durante el periodo de ejecución del servicio:

- 1er Mantenimiento Programado: ejecutarse dentro de los dos últimos meses del primer año del servicio.
- 2do. Mantenimiento Programado: a ejecutarse dentro de los dos últimos meses del segundo año del servicio.
- 3ro. Mantenimiento Programado: a ejecutarse dentro de los dos últimos meses del tercer año del servicio.

Los días y el horario de la ejecución de los mantenimientos serán coordinados con la UIST/OTI, en un horario que no afecte las labores de los usuarios de los servicios internos y externos que brinda el RENIEC.

Los servicios de mantenimientos programados y diagnósticos incluyen: mantenimiento del software de gestión de contenedores, actualización del sistema a la versión recomendada por el fabricante, revisión y afinamiento de configuraciones.

Los trabajos de mantenimiento programado se realizarán de forma remota y estará a cargo del personal clave propuesta para el servicio, y de requerirse un personal que este en el datacenter de RENIEC por alguna actividad especifica, este personal presencial podrá ser propuesto por el contratista.

VII. ENTREGABLES:

La presentación de los entregables se realizará de forma física en la Unidad Ejecutora sito en Av. Canaval y Moreyra Nº 385 Piso 6, San Isidro, Lima o vía mesa de partes virtual de la Unidad Ejecutora 002 (<https://sgd.reniecbid.gob.pe/virtual/inicio.do>) con copia a la mesa de partes virtual del RENIEC (<https://apps.reniec.gob.pe/MesaPartesVirtual/>). Posterior a la aprobación del entregable, este se deberá presentar físicamente en la oficina de la UE002 Proyecto Reniec BID (dirección Av. Canaval y Moreyra Nro. 385, piso 6 San Isidro).


En el siguiente cuadro se detalla los entregables y plazos máximos de entrega que tiene el contratista para cada uno de los entregables, contados a partir del día siguiente de la suscripción del contrato.






Entregable	Denominación	Contiene	% Pago	Plazo de Entrega
01	Plan de Trabajo Proyecto Plataforma de Despliegue del SIIRC	Plan de Trabajo detallado del proyecto que incluya: <ul style="list-style-type: none"> • Insumos requeridos • Revisiones Semanales • Plan de transferencia de conocimiento • Cronograma detallado • Archivo digital ms-project 	2%	Dentro de los quince (15) días calendario, contados a partir del día siguiente de la suscripción del contrato.
02	Entrega de Componentes de la plataforma de despliegue de la arquitectura desacoplada	Se debe incluir lo siguiente: <ul style="list-style-type: none"> • Equipamiento entregado (servidores, sistema de almacenamiento, switches) • Licencias o suscripciones de la plataforma de orquestación de contenedores. • Licencias o suscripciones de las herramientas de la arquitectura desacoplada (API Manager, Streaming de Datos en Tiempo Real, Gestión de Identidades y Control de Accesos) y Base de Datos Oracle. • Diseño de Arquitectura propuesta • Licencias o suscripciones de las herramientas de desarrollo y DevSecOps. • Documentación técnica de compatibilidad de la integración y comunicación de los componentes entregados. 	58%	Dentro de los sesenta (60) días calendario, contados a partir del día siguiente de la aprobación del plan de trabajo
03	Instalación, Configuración de los componentes de la Arquitectura Desacoplada	Informe de Instalación y configuración de los componentes de la arquitectura desacoplada que incluye el equipamiento (servidores, sistema de almacenamiento y switches), software de orquestación de contenedores, herramientas de arquitectura desacoplada (API Manager, Streaming de Datos en Tiempo Real, Gestor de Identidades y Control de Accesos), herramientas de desarrollo y	20%	Dentro de los treinta (30) días calendario, contados a partir de la finalización del Entregable 02.





Entregable	Denominación	Contiene	% Pago	Plazo de Entrega
		devsecops y software de base de datos ORACLE. Se deberá presentar el detalle de las configuraciones realizadas para la instalación y configuración de cada componente.		
04	Implementación y despliegue de Flujo DEVSECOPS	Informe de implementación y despliegue del flujo DEVSECOPS. Se deberá presentar el detalle de las configuraciones realizadas para la implementación del flujo DEVSECOPS. Transferencia de conocimiento, incluir el detalle de la instrucción impartida y las actas de participación del personal.	10%	Dentro de los treinta (30) días calendario, contados a partir de la finalización del Entregable 03.
05	Informe Final y Cierre del proyecto	El detalle de este informe debe estar compuesto por: <ul style="list-style-type: none"> • Documento que detalla el alcance logrado por el proyecto • Resumen ejecutivo • Descripción del trabajo efectuado • Conclusiones del trabajo efectuado • Recomendaciones para el buen uso de la plataforma 	10%	Dentro de los quince (15) días calendario, contados a partir del día siguiente de la finalización del Entregable 04.



VIII. PLAZO DE EJECUCION:

El plazo de ejecución será de ciento cincuenta (150) días calendario, plazo que se considera a partir del día siguiente de la suscripción del contrato. considerando lo establecido en el numeral **VII ENTREGABLES**.

IX. PERFIL DEL CONTRATISTA

Requisitos		Criterio
1	Tipo de contratista	Persona Jurídica

Requisitos		Criterio
2	Experiencia general	<p>Contar con experiencia en venta o comercialización de:</p> <ul style="list-style-type: none"> • Equipamiento informático (servidores, sistemas de almacenamiento, switches) y/o • Software de tipo Middleware (Servidor de Aplicaciones, Servidor ESB, Servidores de Gestión de Colas de Mensajería, servidores de Gestión de Eventos en tiempo real, gestión de APIs, Gestión de Identidades y Control de Accesos) y/o • Software de gestión de contenedores y/o • Servicios de suscripción de soluciones de tipo Middleware (Servidor de Aplicaciones, Servidor ESB, Servidores de Gestión de Colas de Mensajería, servidores de Gestión de Eventos en tiempo real, gestión de APIs, Gestión de Identidades y Control de Accesos) y/o • Servicios de suscripción de software de gestión de contenedores <p>La Persona Jurídica debe estar constituida con una antigüedad no menor de 05 años.</p>
3	Experiencia Específica	<ul style="list-style-type: none"> • Experiencia en venta o comercialización de: <ul style="list-style-type: none"> - Servidores, sistemas de almacenamiento y switches y/o - Software de Orquestación de Contenedores, API Manager, Gestión de Eventos en Tiempo Real, y Gestión de Identidades y Control de Accesos y/o - Base de Datos ORACLE <p>Por un monto no menor de S/ 5,000,000 (cinco millones con 00/100 soles) en los últimos cinco (05) años y mínimo dos contratos en los últimos cinco (05) años.</p> • Acreditar que es canal autorizado de las siguientes soluciones que oferta: <ul style="list-style-type: none"> - Servidores, Sistema de Almacenamiento y switches y/o - Software de Orquestación de contenedores, Software API Manager, software Gestión de Eventos en Tiempo Real, software Gestión de Identidades y Control de Accesos y/o - Software de Base de Datos ORACLE <p>Adjuntando cartas del fabricante (sucursales y/o subsidiarias y/o representante autorizado),</p>



Requisitos		Criterio
		debiendo presentar junto con su propuesta técnica el documento correspondiente que así lo acredite.

X. PERFIL DEL PERSONAL CLAVE

1. Jefe de proyecto:

Requisitos		Criterio
1	Formación académica mínima	<ul style="list-style-type: none"> • Titulado en Ingeniería de Sistemas o Ingeniería Informática o en Ingeniería de Computación y Sistemas o en Ingeniería de Software o Ingeniería de Computación o Ingeniería de similar denominación de las ramas de ciencias de la computación o sistemas o informática. • De preferencia Grado de Maestría en Administración o Maestría en Gestión de Tecnologías de la Información o Maestría en Ingeniería de Sistemas o Maestría en Operaciones o Maestría en Gerencia de Proyectos o similar denominación de las ramas de ciencias de la computación o sistemas o informática o administración u operaciones. • Con Certificación PMP (Project Management Professional) vigente y/o equivalente o Diplomado / Curso de especialización en Gestión de Proyectos con un mínimo de 80 horas.
2	Experiencia profesional mínima	<ul style="list-style-type: none"> • Con experiencia específica, como Gestor o Jefe o Coordinador o Gerente de Proyectos de implementación de orquestación de contenedores y/o Api Manager y/o DevSecOps; en al menos tres (03) proyectos de seis (06) meses de duración mínimo de cada proyecto.
3	Cantidad	01

2. Arquitecto de la Solución:

Requisitos		Criterio
1	Formación académica mínima	<ul style="list-style-type: none"> • Titulado en Ingeniería de Sistemas o Ingeniería Informática o Ingeniería de Computación y Sistemas o Ingeniería de Software o Ingeniería de Computación o Ingeniería Electrónica o Ingeniería



Requisitos		Criterio
		<p>de similar denominación de las ramas de ciencias de la computación o sistemas o informática.</p> <ul style="list-style-type: none"> • Contar con al menos con una certificación oficial en la plataforma de orquestación de contenedores y/o API Manager (o de algún componente de la plataforma API Manager) y/o Gestión de Eventos en Tiempo Real y/o Gestión de Identidades y Control de Accesos, de la solución ofertada.
2	Experiencia profesional mínima	<ul style="list-style-type: none"> • Con experiencia específica, en proyectos de implementación de orquestación de contenedores o API Manager o Gestión de Eventos en Tiempo Real con la solución ofertada; no menor de tres (03) proyectos en los últimos cinco (05) años.
3	Cantidad	01

3. Especialista en Plataforma de Orquestación de Contenedores:

Requisitos		Criterio
1	Formación académica mínima	<ul style="list-style-type: none"> • Titulado en Ingeniería de Sistemas o Ingeniería Informática o Ingeniería de Computación y Sistemas o Ingeniería de Software o Ingeniería de Computación o Ingeniería de similar denominación de las ramas de ciencias de la computación o sistemas o informática. • Contar con la certificación oficial en la plataforma de orquestación de contenedores, de la solución ofertada.
2	Experiencia profesional mínima	<ul style="list-style-type: none"> • Con experiencia específica, en proyectos de implementación de orquestación de contenedores con la solución ofertada; no menor de tres (03) proyectos en los últimos cinco (05) años.
3	Cantidad	01

4. Especialista DevSecOps:

Requisitos		Criterio
1	Formación académica mínima	<ul style="list-style-type: none"> • Titulado en Ingeniería de Sistemas o Ingeniería Informática o Ingeniería de Computación y Sistemas o Ingeniería de Software o Ingeniería de Computación o Ingeniería de similar



Requisitos		Criterio
		denominación de las ramas de ciencias de la computación o sistemas o informática. <ul style="list-style-type: none"> • Con certificación Java. • Con curso en DevSecOps de al menos veinticuatro (24) horas de duración.
2	Experiencia profesional mínima	<ul style="list-style-type: none"> • Con experiencia específica, en proyectos de implementación de DevSecOps o DevOps con la implementación de la herramienta CI/CD y al menos una de las siguientes herramientas: gestor de código fuente y/o gestor de pruebas y/o gestor de análisis estático de código fuente y/o escaneo de vulnerabilidades; no menor de tres (03) proyectos en los últimos cinco (05) años.
3	Cantidad	01

5. Administrador de Base de Datos ORACLE:

Requisitos		Criterio
1	Formación académica mínima	<ul style="list-style-type: none"> • Titulado en Ingeniería de Sistemas o Ingeniería Informática o Ingeniería de Computación y Sistemas o Ingeniería de Software o Ingeniería de Computación o Ingeniería de similar denominación de las ramas de ciencias de la computación o sistemas o informática. • Contar con certificación oficial del fabricante: ORACLE Certified Professional Database 19c Administrator. • Contar con certificación oficial en sistema operativo Linux Empresarial.
2	Experiencia profesional mínima	<ul style="list-style-type: none"> • Con experiencia específica, en proyectos de implementación de servidores de base de datos ORACLE; no menor de tres (03) proyectos en los últimos cinco (05) años.
3	Cantidad	01

XI. LUGAR DE ENTREGA DEL EQUIPO

Los bienes serán entregados al Almacén Central del RENIEC, ubicado en Lima Metropolitana – Perú.

En caso de variarse el lugar de entrega (siempre dentro de Lima Metropolitana) esta será comunicada oportunamente al contratista.

Luego se comunicará al contratista para el traslado (con las medidas de seguridad técnicas, operacional y de transporte con el correspondiente seguro a todo riesgo por cuenta del contratista) al centro de datos que la OTI indique en Lima Metropolitana para su instalación, configuración y puesta en operación.

XII. LUGAR DE PRESTACION DEL SERVICIO

El equipo de trabajo del contratista efectuará el servicio de instalación, configuración y puesta en operación en el centro de datos que la OTI indique en Lima Metropolitana. Las actividades de configuración se podrán hacer de manera presencial y/o remota previa autorización de RENIEC.

XIII. DISPOSICIONES GENERALES:

El RENIEC ha implementado y certificado sus sistemas de gestión en los procesos misionales, tales como:

- a) Sistema de Gestión de Seguridad de la Información alineada a la ISO/IEC 27001:2013
- b) Sistema de Gestión de la Calidad alineada a la ISO 9001:2015
- c) Sistema de Producción de Microformas alineada a la NTP.

El contratista que implemente el servicio se compromete a respetar y aplicar en el servicio brindado, las políticas, procedimientos y controles del Sistema de Gestión, metodología, estándares y otros establecidos por el RENIEC.

El Servicio no implica pago adicional alguno a los contenidos en la presente EETT, debiendo el proveedor asumir todos los costos a generarse para la obtención de los productos.

XIV. RESPONSABILIDAD DEL CONTRATISTA

En atención a lo previsto en el Contrato de Préstamo y en las políticas para la contratación de consultores, el contratista asume la responsabilidad en ejecutar el servicio a su cargo con la debida diligencia y conforme a las normas vigentes para la prestación del servicio, incluyendo la presentación oportuna de los productos respectivos, estableciéndose que su responsabilidad, en caso de incumplimiento, ascenderá hasta la totalidad de los pagos derivados de la ejecución del servicio a su cargo.

El contratista tiene la facultad de contratar personal adicional al personal clave para ejecutar el servicio y lograr la entrega oportuna de los productos.

En la propuesta técnica se debe presentar documentación técnica que acredite la compatibilidad de la integración y comunicación de los componentes de la plataforma de despliegue de la arquitectura desacoplada.



El contratista, es el responsable absoluto por la calidad ofrecida y por los vicios ocultos de los bienes o servicios ofertados por un plazo no menor a 1 (uno) año contado a partir de la conformidad otorgada por la Unidad Ejecutora 002: RENIEC BID.

XV. COORDINACION, SUPERVISION Y CONFORMIDAD

La coordinación y supervisión será responsabilidad del Equipo Técnico de Trabajo, conformado por representantes de la unidad ejecutora del proyecto y del RENIEC.

La conformidad será emitida por la Oficina de Tecnologías de la Información, previo informe técnico de la Unidad de Infraestructura y Soporte Técnico.

La aprobación u observación de los entregables se va a realizar en cinco (05) días útiles por el RENIEC, en caso de ser observado, deberá ser corregido en tres (03) días útiles por el contratista.

XVI. CONFIDENCIALIDAD DE LA INFORMACIÓN / PROPIEDAD INTELECTUAL

Toda información a la que tenga acceso el proveedor, así como su personal, es estrictamente confidencial. El proveedor y su personal designado al servicio deben comprometerse a mantener las reservas del caso y no transmitir a ninguna persona (natural o jurídica) sin autorización expresa y por escrito del RENIEC.

Todos los derechos intelectuales de los entregables serán de propiedad del RENIEC desde el día de su presentación y no podrán ser usados para otro fin que no sea la presente contratación sin autorización expresa y por escrito.

XVII. PENALIDADES

Entrega retrasada injustificada de entregables (aplicable según plazos de entrega señalados en el numeral VII del presente documento)

En caso que el contratista incurra en el retraso injustificado en la ejecución de las prestaciones del servicio, de acuerdo a los plazos estipulados en la presente EETT, la Unidad Ejecutora aplicaría una penalidad de aplicación automática por cada día calendario de retraso, hasta por un monto máximo equivalente al diez por ciento (10%) del monto global contratado, de llegar al valor total del 10% se podrá resolver el contrato por incumplimiento y a comunicar a las autoridades competentes correspondientes al BID y a la autoridad que rige el Sistema Nacional de las Contrataciones en el Estado Peruano.

La penalidad establecida en la presente cláusula se aplicará sin perjuicio de la obligación del contratista de responder por los daños y perjuicios que pudieran derivarse de su incumplimiento o de las demás sanciones que pudieran corresponder.

Dicha penalidad por día calendario de atraso se calculará de acuerdo con la siguiente fórmula:



$$\text{Penalidad diaria} = \frac{0.10 \times \text{monto}}{0.25 \times \text{plazo en días}}$$

Dónde:

Monto = monto del entregable en el contrato

Plazo en días = plazo máximo de entrega de cada entregable.

XVIII. ANEXOS



ANEXO 01
ESPECIFICACIONES TECNICAS DEL HARDWARE PARA LA PLATAFORMA DE
ORQUESTACIÓN DE CONTENEDORES PARA LOS AMBIENTES DE
DESARROLLO, INTEGRACIÓN Y PRUEBAS DEL SIIRC

La infraestructura base solicitada para implementar la plataforma de orquestación de contenedores para los ambientes de desarrollo, integración y pruebas debe tener las siguientes especificaciones:

El hardware requerido para la plataforma de orquestación de contenedores para los ambientes de desarrollo, integración y pruebas del SIIRC deberá ser instalado íntegramente en un único rack. Este rack deberá ser estándar de 42 RU y contar con espacio suficiente para garantizar una instalación segura y adecuada, incluyendo las conexiones eléctricas, de datos, accesorios y demás elementos necesarios para el correcto funcionamiento. El contratista deberá proporcionar tanto el rack como todos los componentes necesarios para la instalación, configuración e interconexión a la red del RENIEC.

HARDWARE

CARACTERISTICAS	
Nodos Maestros (03 unidades)	Priorización
Servidor Rackeable	Obligatorio
Dos (02) procesadores por nodo con fecha de lanzamiento a partir del Q1 del 2024 Cada procesador debe tener (16 cores, 2.8 GHz, 37.5 MB de cache L3, 195 Watts) como mínimo	Obligatorio
12 módulos de 32 GB de 5600 MHz tipo RDIMM, de tecnología ECC	Obligatorio
Mínimo 04 puertos Ethernet de 10/25Gb SFP+ (LAN) incluyendo 04 Transceiver de 10Gb Mínimo 02 puertos Ethernet RJ45 de 1Gb Mínimo 02 puertos Fibre Channel 32 Gb 2 puertos PCIe V2	Obligatorio
Cuatro (04) disco de SSD 3,84 TB, lecturas intensivas, SATA 6 Gb de intercambio en caliente	Obligatorio
Dos (02) fuentes de poder tipo Hot Swap redundantes y de 1,100W Platinum (230V) como mínimo	Obligatorio
Todos los componentes, partes y/o piezas, cables y accesorios, deben ser originales y mínimamente fabricados el año 2024	Obligatorio
- Soporte de TPM 2.0. - El servidor debe cumplir con el NIST SP 800-147B.	Obligatorio



CARACTERISTICAS	
Nodos Maestros (03 unidades)	Priorización
<p>- Sistema de arranque (boot) seguro, que garantice que solo se cargue software inmutable y firmado durante el tiempo de arranque, evitando que se cargue código malicioso y ayudando a prevenir ataques como la instalación de rootkits.</p> <p>- Protección contra actualizaciones de firmware no autorizadas y corrupción, restaurando el firmware a un estado integral y monitoreo del firmware en busca de posibles compromisos de ataques cibernéticos. Contar con procesos de firma de firmware que cumplen con los requisitos de FIPS y NIST.</p>	
<p>El servidor debe de tener:</p> <p>Certificado de no perjudicar la salud y/o presentar un impacto negativo al medio ambiente EPEAT.</p> <p>Certificado de eficiencia de energía (Energy Star).</p>	Obligatorio
<p>Software de Administración que permita lo siguiente:</p> <ul style="list-style-type: none"> • Administración centralizada de todos los dispositivos desde una única interfaz • La gestión de inventarios y el seguimiento de activos de hardware • Actualizaciones de firmware de manera centralizada, asegurando que todos los dispositivos estén ejecutando las versiones más recientes y seguras • Programar actualizaciones fuera de horario para minimizar el impacto en las operaciones • Integración con otras herramientas de gestión y orquestación, mínimamente con las herramientas ofertadas • Aplicación para la administración remota, permitiendo a los administradores supervisar y gestionar la infraestructura desde cualquier lugar. • Alertas en tiempo real, vistas del estado del sistema y capacidades de resolución de problemas • Arquitectura sin agentes externos. • Proporcionar datos para mejorar la eficiencia operativa de la infraestructura • Informes detallados y cuadros de mando (dashboards) personalizables que permiten a los administradores obtener una visión completa del rendimiento y la salud de la infraestructura 	Obligatorio
<p>- La garantía y soporte debe ser por tres (03) años y estar disponible las 24 horas de los 07 días de la semana, incluido feriados, durante el período de 03 años con tiempo de respuesta de 04 horas por parte del contratista y del fabricante</p>	Obligatorio





CARACTERISTICAS	
Nodos Maestros (03 unidades)	Priorización
<ul style="list-style-type: none">- RMA (Return Merchandise Authorization), es decir autorización de devolución de mercancía: El contratista como parte del soporte y garantía ofertada, debe incluir el suministro de equipos en calidad de RMA por el periodo de tres (03) años, para el reemplazo respectivo de los mismos, cuando el equipo quede en estado inoperativo y sin diagnostico por más de 72 horas, se debe reemplazar el equipo por parte del contratista y/o fabricante- El plazo de reemplazo del hardware será de 15 días calendarios como máximo- El equipamiento debe contar con Soporte técnico del fabricante para hardware y/o software a través de una línea gratuita 0-800- Deberá permitir el registro de solicitudes de soporte a través de un portal web del contratista y/o fabricante para el seguimiento y control de los incidentes y/o requerimientos- El soporte y la garantía podrá ser atendida de manera remota y/o presencial en coordinación con el RENIEC- El contratista deberá presentar una carta del fabricante confirmando lo solicitado, esta carta debe ser presentada al entregar el equipamiento, asimismo, la carta deberá considerar la Disponibilidad de Upgrade, parches del software para el equipo- La garantía y soporte iniciará a partir del día siguiente de la entrega de las licencias.- La carta de garantía emitida por el fabricante o sucursal del fabricante por tres (03) años en partes, mano de obra y on site para todas sus partes y componentes por defectos de fábrica, contados a partir del día siguiente de instalación y configuración.	



CARACTERISTICAS	
Nodos Worker (03 unidades)	Priorización
Servidor Rackeable	Obligatorio
Dos (02) procesadores por nodo con fecha de lanzamiento a partir del Q1 del 2024 Cada procesador debe tener (16 cores, 2.8 GHz, 37.5 MB de cache L3, 195 Watts) como mínimo	Obligatorio
8 módulos de 32GB de 5600 MHz tipo RDIMM como mínimo, de tecnología ECC.	Obligatorio
Mínimo 04 puertos Ethernet de 10/25Gb SFP+ (LAN) incluyendo 04 Transceiver de 10Gb	Obligatorio



CARACTERISTICAS	
Nodos Worker (03 unidades)	Priorización
Mínimo 02 puertos Ethernet RJ45 de 1Gb Mínimo 02 puertos Fibre Channel 32 Gb 2 puertos PCIe V2	
Cuatro (04) disco de SSD 3,84 TB, lecturas intensivas, SATA 6 Gb de intercambio en caliente	Obligatorio
Dos (02) fuentes de poder tipo Hot Swap redundantes y de 1,100W Platinum (230V) como mínimo	Obligatorio
- Soporte de TPM 2.0.- El servidor debe cumplir con el NIST SP 800-147B. - Sistema de arranque (boot) seguro, que garantice que solo se cargue software inmutable y firmado durante el tiempo de arranque, evitando que se cargue código malicioso y ayudando a prevenir ataques como la instalación de rootkits. - Protección contra actualizaciones de firmware no autorizadas y corrupción, restaurando el firmware a un estado integral y monitoreo del firmware en busca de posibles compromisos de ataques cibernéticos. Contar con procesos de firma de firmware que cumplen con los requisitos de FIPS y NIST.	Obligatorio
El servidor debe de tener: Certificado de no perjudicar la salud y/o presentar un impacto negativo al medio ambiente EPEAT. Certificado de eficiencia de energía (Energy Star).	Obligatorio
Software de Administración que permita lo siguiente: <ul style="list-style-type: none">• Administración centralizada de todos los dispositivos desde una única interfaz• La gestión de inventarios y el seguimiento de activos de hardware• Actualizaciones de firmware de manera centralizada, asegurando que todos los dispositivos estén ejecutando las versiones más recientes y seguras• Programar actualizaciones fuera de horario para minimizar el impacto en las operaciones• Integración con otras herramientas de gestión y orquestación, mínimamente con las herramientas ofertadas• Aplicación para la administración remota, permitiendo a los administradores supervisar y gestionar la infraestructura desde cualquier lugar• Alertas en tiempo real, vistas del estado del sistema y capacidades de resolución de problemas• Arquitectura sin agentes externos• Proporcionar datos para mejorar la eficiencia operativa de la infraestructura	Obligatorio





CARACTERISTICAS	
Nodos Worker (03 unidades)	Priorización
<ul style="list-style-type: none">• Informes detallados y cuadros de mando (dashboards) personalizables que permiten a los administradores obtener una visión completa del rendimiento y la salud de la infraestructura	
Todos los componentes, partes y/o piezas, cables y accesorios, deben ser originales y mínimamente fabricados el año 2024	Obligatorio
<ul style="list-style-type: none">- La garantía y soporte debe ser por tres (03) años y estar disponible las 24 horas de los 07 días de la semana, incluido feriados, durante el período de 03 años con tiempo de respuesta de 04 horas por parte del contratista y del fabricante- RMA (Return Merchandise Authorization), es decir autorización de devolución de mercancía: El contratista como parte del soporte y garantía ofertada, debe incluir el suministro de equipos en calidad de RMA por el periodo de tres (03) años, para el reemplazo respectivo de los mismos, cuando el equipo quede en estado inoperativo y sin diagnostico por más de 72 horas, se debe reemplazar el equipo por parte del contratista y/o fabricante- El plazo de reemplazo del hardware será de 15 días calendarios como máximo- El equipamiento debe contar con Soporte técnico del fabricante para hardware y/o software a través de una línea gratuita 0-800- Deberá permitir el registro de solicitudes de soporte a través de un portal web del contratista y/o fabricante para el seguimiento y control de los incidentes y/o requerimientos- El soporte y la garantía podrá ser atendida de manera remota y/o presencial en coordinación con el RENIEC- El contratista deberá presentar una carta del fabricante confirmando lo solicitado, esta carta debe ser presentada al entregar el equipamiento, asimismo, la carta deberá considerar la Disponibilidad de Upgrade, parches del software para el equipo- La garantía y soporte iniciará a partir del día siguiente de la entrega de las licencias.- La carta de garantía emitida por el fabricante o sucursal del fabricante por tres (03) años en partes, mano de obra y on site para todas sus partes y componentes por defectos de fábrica, contados a partir del día siguiente de instalación y configuración.	Obligatorio





ALMACENAMIENTO		
CARACTERÍSTICAS	DESCRIPCIÓN	Priorización
Cantidad	- Una (01) unidad	Obligatorio
Factor de forma	Rackeable	Obligatorio
Módulo de Control	<ul style="list-style-type: none"> - Dos (02) módulos de control o dos (02) controladoras redundantes activo-activo. - El módulo de control deberá contar como mínimo con memoria caché de 256 GB mínimo. - El módulo de control deberá contar como mínimo con cuatro (04) puertos FC de 32 Gbps, cuatro (04) puertos por controlador - Deberá incluir un cable LC-LC multimodo de 3 y/o 5 metros por cada puerto - Deberán contar con 24 bahías para alojar discos de 2.5" 	Obligatorio
Módulos NVMe	- Discos SSD FLASH CORE MODULE NVME o SFF SSD de tipo NVMe de 15.36 TB de capacidad física configurados en RAID 6 Distribuido (incluido un módulo en Hot Spare)	Obligatorio
Capacidad de almacenamiento	<ul style="list-style-type: none"> - Almacenamiento no menor de 300 TB usables. - Capacidad de crecimiento de almacenamiento debe ser hasta 500 TB como mínimo. 	Obligatorio
Energía	- Cuatro (04) fuentes de alimentación con sus respectivos cables de energía (C19 a C20)	Obligatorio
Gestión	- Mediante una interfaz gráfica de usuario (GUI)	Obligatorio
Software	- Deberá incluir la licencia de administración con tres (03) años de mantenimiento de software	Obligatorio
Año de Fabricación	- Todos los componentes, partes y/o piezas, cables y accesorios, deben ser originales y mínimamente fabricados el año 2024, para lo cual el contratista deberá presentar una carta del fabricante y/o subsidiaria local y/o subsidiaria regional confirmando lo solicitado, esta carta debe ser presentada al entregar el equipamiento	Obligatorio





ALMACENAMIENTO		
CARACTERÍSTICAS	DESCRIPCIÓN	Priorización
Garantía y Soporte	<ul style="list-style-type: none">- La garantía y soporte debe ser por tres (03) años y estar disponible las 24 horas de los 07 días de la semana, incluido feriados, durante el período de 03 años con tiempo de respuesta de 04 horas por parte del contratista y del fabricante- RMA (Return Merchandise Authorization), es decir autorización de devolución de mercancía: El contratista como parte del soporte y garantía ofertada, debe incluir el suministro de equipos en calidad de RMA por el periodo de tres (03) años, para el reemplazo respectivo de los mismos, cuando el equipo quede en estado inoperativo y sin diagnostico por más de 72 horas, se debe reemplazar el equipo por parte del contratista y/o fabricante- El plazo de reemplazo del hardware será de 15 días calendarios como máximo- El equipamiento debe contar con Soporte técnico del fabricante para hardware y/o software a través de una línea gratuita 0-800- Deberá permitir el registro de solicitudes de soporte a través de un portal web del contratista y/o fabricante para el seguimiento y control de los incidentes y/o requerimientos- El soporte y la garantía podrá ser atendida de manera remota y/o presencial en coordinación con el RENIEC- El contratista deberá presentar una carta del fabricante confirmando lo solicitado, esta carta debe ser presentada al entregar el equipamiento, asimismo, la carta deberá considerar la Disponibilidad de Upgrade, parches del software para el equipo- La garantía y soporte iniciará a partir del día siguiente de la entrega de las licencias.- La carta de garantía emitida por el fabricante o sucursal del fabricante por tres (03) años en partes, mano de obra y on site para todas sus partes y componentes por defectos de fábrica, contados a partir del día siguiente de instalación y configuración.	Obligatorio





ALMACENAMIENTO		
CARACTERÍSTICAS	DESCRIPCIÓN	Priorización
Respecto a los componentes	- El contratista al momento de entregar el equipo deberá de evidenciar y/o adjuntar la documentación que sustente y confirme el cumplimiento de las características de todos los componentes requeridos	Obligatorio
Rotulado y Etiquetado	- El contratista deberá de realizar el rotulado y etiquetado necesario para la identificación de los equipos y conexiones previa coordinación con el RENIEC	Obligatorio
Ordenamiento de cableado	- El proveedor deberá de organizar los cables de conexión que el equipamiento requiera con cinta adhesiva hook and loop de color negro	Obligatorio
Rackeo de sistema de almacenamiento	- Deberá incluir kits para rackeo y/o accesorios necesarios para su instalación en el gabinete que el RENIEC especifique al contratista.	Obligatorio



SWITCH PARA CONECTIVIDAD DE COMPONENTES		
CARACTERISTICA	DETALLE	Priorización
Puertos de Acceso	24 puertos de 10/25 Gbps SFP+	Obligatorio
Puerto de Administración	1 puerto RJ-45 10/100/1000 Mbps	Obligatorio
Fuentes de Alimentación	2 fuentes de alimentación redundantes (hot-swappable)	Obligatorio
Capacidad de Switching	≥ 2.0 Tbps	Obligatorio
Capacidad de Reenvío	≥ 450 Mpps	Obligatorio
Latencia	≤ 1 microsegundo	Obligatorio
Buffer de Paquetes	≥ 16 MB	Obligatorio
Memoria Flash	≥ 2 GB	Obligatorio
DRAM	≥ 8GB	Obligatorio



SWITCH PARA CONECTIVIDAD DE COMPONENTES		
CARACTERISTICA	DETALLE	Priorización
Velocidades de Transmisión	10 Gbps, 25 Gbps	Obligatorio
Capacidad VLAN	4040 vlans o superior.	Obligatorio
Encapsulamiento VLAN	802.1Q	Obligatorio
Soporte de Capa 2	Sí	Obligatorio
Soporte de Capa 3	Sí (Routing estático y dinámico)	Obligatorio
Protocolos de Enrutamiento	OSPF, BGP, RIP, (EIGRP opcional)	Obligatorio
Seguridad	ACLs, listas de control de acceso, autenticación RADIUS/TACACS+	Obligatorio
QoS	Sí, con soporte para políticas avanzadas	Obligatorio
Multicast	Soporte para IGMP, PIM	Obligatorio
Gestión	CLI, SNMP, RMON, Syslog, Telnet, SSH, GUI web	Obligatorio
Funciones Avanzadas	VXLAN, (MPLS opcional), EVPN	Obligatorio
Consumo de Energía	Max: 586 W	Obligatorio
Temperatura de Operación	0 a 40 °C	Obligatorio
Humedad Relativa de Operación	10% a 90% sin condensación	Obligatorio
Certificaciones	(CE Opcional), FCC, UL, RoHS	Obligatorio
Garantía y soporte	<ul style="list-style-type: none"> - La garantía y soporte debe ser por tres (03) años y estar disponible las 24 horas de los 07 días de la semana, incluido feriados, durante el período de 03 años con tiempo de respuesta de 04 horas por parte del contratista y del fabricante - RMA (Return Merchandise Authorization), es decir autorización de devolución de mercancía: El contratista como parte del 	Obligatorio





SWITCH PARA CONECTIVIDAD DE COMPONENTES		
CARACTERISTICA	DETALLE	Priorización
	<p>soporte y garantía ofertada, debe incluir el suministro de equipos en calidad de RMA por el periodo de tres (03) años, para el reemplazo respectivo de los mismos, cuando el equipo quede en estado inoperativo y sin diagnostico por más de 72 horas, se debe reemplazar el equipo por parte del contratista y/o fabricante</p> <ul style="list-style-type: none">- El plazo de reemplazo del hardware será de 15 días calendarios como máximo- El equipamiento debe contar con Soporte técnico del fabricante para hardware y/o software a través de una línea gratuita 0-800- Deberá permitir el registro de solicitudes de soporte a través de un portal web del contratista y/o fabricante para el seguimiento y control de los incidentes y/o requerimientos- El soporte y la garantía podrá ser atendida de manera remota y/o presencial en coordinación con el RENIEC- El contratista deberá presentar una carta del fabricante confirmando lo solicitado, esta carta debe ser presentada al entregar el equipamiento, asimismo, la carta deberá considerar la Disponibilidad de Upgrade, parches del software para el equipo- La garantía y soporte iniciará a partir del día siguiente de la entrega de las licencias.- La carta de garantía emitida por el fabricante o sucursal del fabricante por tres (03) años en partes, mano de obra y on site para todas sus partes y componentes por defectos de fábrica, contados a partir del día siguiente de instalación y configuración.	



SWITCH PARA CONECTIVIDAD CON SISTEMA DE ALMACENAMIENTO		
ESPECIFICACIÓN	DETALLE	Priorización
Puertos Activos	24 puertos de 32 Gbps Fiber Channel SFP+, licenciados activados y con su respectivo transceiver	Obligatorio



SWITCH PARA CONECTIVIDAD CON SISTEMA DE ALMACENAMIENTO		
ESPECIFICACIÓN	DETALLE	Priorización
Expansión de Puertos	Hasta 48 puertos de 32 Gbps Fiber Channel	Obligatorio
Puerto de Administración	1 puerto RJ-45 10/100/1000 Mbps	Obligatorio
Fuentes de Alimentación	2 fuentes de alimentación redundantes (hot-swappable)	Obligatorio
Ancho de banda agregado	2 Tbps	Obligatorio
Tamaño máximo de frame	2,112-byte	Obligatorio
Latencia	≤ 780 nanosegundos (FC a FC)	Obligatorio
Velocidades de Transmisión	32 Gbps, auto-negociable con 8, 16 Gbps	Obligatorio
Capacidad de nodos activos	6000	Obligatorio
Seguridad	Zoning, autenticación RADIUS/TACACS+, LDAP, OpenLDAP, Port Binding	Obligatorio
QoS	Sí, con soporte para políticas avanzadas	Obligatorio
Gestión	CLI, SNMP, RMON, Syslog, Telnet, SSH, GUI web	Obligatorio
Funciones Avanzadas Incluidas	Virtual SANs (VSANs), NPIV, FCoE, Fabric Vision	Obligatorio
Fuentes de Poder	Redundantes de 250W hot-swap.	Obligatorio
Temperatura de Operación	0 a 40 °C	Obligatorio
Humedad Relativa de Operación	8% a 90% sin condensación	Obligatorio
Certificaciones	EN 55022, FCC, UL, RoHS	Obligatorio
Garantía y soporte	<ul style="list-style-type: none"> - La garantía y soporte debe ser por tres (03) años y estar disponible las 24 horas de los 07 días de la semana, incluido feriados, durante el período de 03 años con tiempo de respuesta de 04 horas por parte del contratista y del fabricante - RMA (Return Merchandise Authorization), es decir autorización de devolución de 	Obligatorio





SWITCH PARA CONECTIVIDAD CON SISTEMA DE ALMACENAMIENTO		
ESPECIFICACIÓN	DETALLE	Priorización
	<p>mercancía: El contratista como parte del soporte y garantía ofertada, debe incluir el suministro de equipos en calidad de RMA por el periodo de tres (03) años, para el reemplazo respectivo de los mismos, cuando el equipo quede en estado inoperativo y sin diagnostico por más de 72 horas, se debe reemplazar el equipo por parte del contratista y/o fabricante</p> <ul style="list-style-type: none">- El plazo de reemplazo del hardware será de 15 días calendarios como máximo- El equipamiento debe contar con Soporte técnico del fabricante para hardware y/o software a través de una línea gratuita 0-800- Deberá permitir el registro de solicitudes de soporte a través de un portal web del contratista y/o fabricante para el seguimiento y control de los incidentes y/o requerimientos- El soporte y la garantía podrá ser atendida de manera remota y/o presencial en coordinación con el RENIEC- El contratista deberá presentar una carta del fabricante confirmando lo solicitado, esta carta debe ser presentada al entregar el equipamiento, asimismo, la carta deberá considerar la Disponibilidad de Upgrade, parches del software para el equipo- La garantía y soporte iniciará a partir del día siguiente de la entrega de las licencias.- La carta de garantía emitida por el fabricante o sucursal del fabricante por tres (03) años en partes, mano de obra y on site para todas sus partes y componentes por defectos de fábrica, contados a partir del día siguiente de instalación y configuración.	



ANEXO 02
ESPECIFICACIONES TECNICAS DE LA PLATAFORMA DE ORQUESTACIÓN DE
CONTENEDORES PARA LOS AMBIENTES DE DESARROLLO, INTEGRACIÓN Y
PRUEBAS DEL SIIRC

La implementación del SIIRC se va a realizar utilizando la tecnología JAVA, en consecuencia, la plataforma de orquestación de contenedores para los ambientes de desarrollo, integración y pruebas deben soportar dicha tecnología.

La plataforma de orquestación de contenedores para los ambientes de desarrollo, integración y pruebas debe tener las siguientes especificaciones:

ASPECTO	CARACTERÍSTICAS	PRIORIZACIÓN
Plataforma de Orquestación	- Automatización de despliegues: Permite la rápida implementación y gestión de aplicaciones en contenedores, facilitando la entrega continua y reduciendo el tiempo de despliegue	Obligatorio
	- Escalabilidad elástica: Proporciona una infraestructura que puede adaptarse dinámicamente a las demandas de carga de trabajo, escalando automáticamente para satisfacer las necesidades del SIIRC sin interrupciones en el servicio	Obligatorio
	- Gestión centralizada: Ofrece una interfaz centralizada para administrar y supervisar todos los aspectos de los contenedores y las aplicaciones desplegadas, simplificando la operación y la resolución de problemas	Obligatorio
	- Despliegue multi-nube: Permite implementar y gestionar aplicaciones en múltiples entornos de nube, incluyendo nubes públicas, privadas e híbridas, proporcionando flexibilidad y portabilidad para las cargas de trabajo del SIIRC	Deseable
	- Despliegue automatizado: Utiliza herramientas de automatización para implementar y configurar rápidamente la infraestructura de hardware requerida para la plataforma de orquestación de contenedores, agilizando el proceso de implementación y reduciendo los errores humanos	Obligatorio





ASPECTO	CARACTERÍSTICAS	PRIORIZACIÓN
	- Plataforma integrada: Debe permitir la integración con bases de datos, servicios de mensajería y análisis de datos	Obligatorio
	- Gestión de políticas avanzada: Permite definir y aplicar políticas de seguridad, cumplimiento y gobernanza de manera centralizada, garantizando el cumplimiento de los requisitos regulatorios y la seguridad de los datos todo momento	Obligatorio
Infraestructura de Hardware	- Alta disponibilidad: Utiliza tecnologías de redundancia y failover para garantizar la disponibilidad continua de los servicios, minimizando los tiempos de inactividad y asegurando la continuidad operativa del SIIRC	Obligatorio
	- Rendimiento optimizado: Optimización de la configuración de hardware para ofrecer un rendimiento óptimo y una capacidad de respuesta rápida, asegurando una experiencia de usuario fluida y eficiente	Obligatorio
	- Escalabilidad: Permite agregar recursos de hardware automáticamente para manejar cargas de trabajo crecientes, garantizando un rendimiento consistente incluso en momentos de alta demanda	Obligatorio
	- Capacidad para realizar la instalación y configuración directamente sobre los servidores sin necesidad de contar con algún software de virtualización o hipervisor.	Obligatorio
Integración de Herramientas DevOpsSec	- Habilitación de operadores y componentes específicos de DevOpsSec en la plataforma para fortalecer la seguridad y la gestión del ciclo de vida del software	Obligatorio
	- Configuración de herramientas de seguridad como escaneo de vulnerabilidades, gestión de secretos y detección de intrusiones para proteger las aplicaciones desplegadas en la plataforma	Obligatorio
	- Automatización de procesos de seguridad, como pruebas de penetración, análisis estático	Obligatorio



ASPECTO	CARACTERÍSTICAS	PRIORIZACIÓN
	y dinámico de código, y cumplimiento de políticas de seguridad, para garantizar la integridad y la conformidad de las aplicaciones	
	- Implementación de herramientas de gestión de riesgos que identifiquen y mitiguen posibles amenazas y vulnerabilidades en las aplicaciones desplegadas, reduciendo la exposición a riesgos de seguridad	Obligatorio
	- Establecimiento de mecanismos de monitoreo continuo que alerten sobre actividades sospechosas o incidentes de seguridad, permitiendo una respuesta rápida y eficaz a posibles amenazas	Obligatorio
	- Integración de prácticas de seguridad en los procesos DevSecOps, asegurando que la seguridad sea una consideración integral en todas las etapas del ciclo de vida del desarrollo de software	Obligatorio
	- Implementación de mejoras continuas en la seguridad basadas en análisis de riesgos, evaluaciones de seguridad y retroalimentación del equipo de operaciones de seguridad	Obligatorio
	- Entorno seguro por defecto: Ofrece una arquitectura segura por diseño que protege las aplicaciones contra amenazas conocidas y desconocidas desde el momento del despliegue, minimizando la superficie de ataque y reduciendo la exposición a vulnerabilidades	Obligatorio
	- Integración con herramientas de seguridad en cluster: Proporciona una solución de seguridad nativa que protege proactivamente las aplicaciones y los datos del SIIRC contra amenazas cibernéticas, detectando y respondiendo automáticamente a ataques en tiempo real, sin impactar la productividad del desarrollo	Obligatorio



ASPECTO	CARACTERÍSTICAS	PRIORIZACIÓN
	<ul style="list-style-type: none"> - Cumplimiento continuo: Facilita la auditoría y el cumplimiento normativo al ofrecer informes detallados sobre el estado de seguridad de las aplicaciones, permitiendo a los equipos de seguridad demostrar el cumplimiento de los requisitos regulatorios y las mejores prácticas de seguridad 	Obligatorio
Documentación	<ul style="list-style-type: none"> - Recursos de aprendizaje: Proporciona una variedad de recursos, como documentación técnica y tutoriales en línea para el uso y la administración de la plataforma 	Obligatorio
	<ul style="list-style-type: none"> - Soporte técnico: Ofrece servicios de soporte técnico especializado, incluyendo asistencia telefónica, chat en línea y asesoramiento personalizado, para resolver dudas, problemas y proporcionar orientación técnica durante la implementación y la operación de la plataforma 	Obligatorio
Compatibilidad y Conformidad	<ul style="list-style-type: none"> - Conformidad con estándares: Cumple con los estándares técnicos y de seguridad reconocidos por la industria y las regulaciones gubernamentales, garantizando la conformidad con los requisitos de cumplimiento y la interoperabilidad con sistemas externos 	Obligatorio
	<ul style="list-style-type: none"> - Actualizaciones y parches regulares: Proporciona actualizaciones regulares de software y parches de seguridad, asegurando la protección continua contra amenazas y vulnerabilidades, y manteniendo la plataforma alineada con las últimas innovaciones tecnológicas 	Obligatorio
	<ul style="list-style-type: none"> - Soporte a largo plazo: Ofrece un ciclo de vida de soporte extendido que garantiza actualizaciones de seguridad y correcciones de errores durante un período prolongado, proporcionando estabilidad y confiabilidad a largo plazo para las operaciones del SIIRC 	Obligatorio
	<ul style="list-style-type: none"> - Validación de certificaciones: Ha obtenido certificaciones de conformidad con estándares de la industria y regulaciones gubernamentales, incluyendo ISO, SOC y 	Obligatorio



ASPECTO	CARACTERÍSTICAS	PRIORIZACIÓN
	FedRAMP, que demuestran su compromiso con la calidad, la seguridad y el cumplimiento normativo en entornos gubernamentales.	
Monitoreo y Optimización	- Implementación de soluciones de monitoreo y registro que permitan supervisar el desempeño de la plataforma de orquestación de contenedores en tiempo real	Obligatorio
	- Optimización de la Configuración inicial para asegurar un rendimiento óptimo y detectar posibles problemas antes de que afecten a la operación	Obligatorio
	- Plataforma de monitorización integrada: Ofrece herramientas nativas de monitorización y análisis, como Prometheus y Grafana, que proporcionan métricas detalladas y visualizaciones gráficas del rendimiento de la plataforma y las aplicaciones desplegadas, facilitando la detección temprana de problemas y la optimización continua	Obligatorio
	- Automatización de la optimización de rendimiento: Utiliza tecnologías de autoscaling y ajuste dinámico de recursos para optimizar automáticamente la asignación de recursos en función de las demandas de carga de trabajo, mejorando la eficiencia operativa y reduciendo los costos de infraestructura.	Obligatorio
Seguridad y Cumplimiento	- Implementación de políticas de seguridad y controles de acceso para proteger los datos y las aplicaciones del SIIRC contra amenazas internas y externas	Obligatorio
	- Enfoque de seguridad integral: Ofrece una arquitectura de seguridad en capas que protege las aplicaciones y los datos en todas las etapas del ciclo de vida, desde el desarrollo hasta la producción, garantizando la confidencialidad, integridad y disponibilidad de la información	Obligatorio
	- Cumplimiento continuo: Facilita la auditoría y el cumplimiento normativo al ofrecer informes detallados sobre el estado de seguridad de las	Obligatorio



ASPECTO	CARACTERÍSTICAS	PRIORIZACIÓN
	aplicaciones del SIIRC, permitiendo a los equipos de seguridad demostrar el cumplimiento de los requisitos regulatorios y las mejores prácticas de seguridad.	

El contratista deberá brindar licenciamiento o suscripción de la herramienta de orquestación de contenedores ofertada por el periodo de 03 años, contabilizados a partir del día siguiente de la entrega de las licencias o suscripciones. La herramienta de orquestación de contenedores deberá coberturar el licenciamiento o suscripción para la totalidad de los cores de los nodos workers de los servidores ofertados en el Anexo 01.



ANEXO 03
ESPECIFICACIONES TÉCNICAS DE LAS HERRAMIENTAS DE DESARROLLO Y
DEVSECOPS PARA LOS AMBIENTES DE DESARROLLO, INTEGRACIÓN Y
PRUEBAS DEL SIIRC

En la implementación del SIIRC se debe considerar la seguridad y privacidad desde el diseño para lo cual se debe integrar consideraciones de seguridad y privacidad aplicando el principio de “privacidad por diseño” mediante la encriptación de datos, gestión de identidades y accesos, y el cumplimiento de normativas.

Se requiere diseñar una solución integral de DevSecOps, como un sistema integrado con la finalidad de mejorar la eficiencia y el rendimiento del ciclo de vida de los microservicios y sus contenedores.

La implementación del SIIRC se va a realizar utilizando la tecnología JAVA, en consecuencia, las herramientas de desarrollo y DevSecOps deben soportar dicha tecnología.

Las herramientas para implementar DevSecOps para los ambientes de desarrollo, integración y pruebas deben tener las siguientes especificaciones:

HERRAMIENTA	CARACTERÍSTICAS	PRIORIZACIÓN
Gestor de código fuente	- Distribuido y Descentralizado: permite trabajar de forma independiente y fusionar los cambios en el repositorio principal de manera eficiente	Obligatorio
	- Rastreo Preciso de Cambios: realizar un seguimiento preciso de los cambios realizados en cada archivo a lo largo del tiempo, permitiendo ver el historial completo de cambios, incluidas las diferencias entre versiones y la posibilidad de regresar a versiones anteriores en caso de problemas	Obligatorio
	- Ramificación Eficiente: permite la creación y gestión de ramas, fomentando el desarrollo paralelo y facilita la colaboración en equipos grandes	Obligatorio
	- Fusiones Simplificadas: permite la capacidad de fusionar cambios entre diferentes ramas, combinando cambios de manera eficiente, lo que facilita la integración continua y evita conflictos de código.	Obligatorio





HERRAMIENTA	CARACTERÍSTICAS	PRIORIZACIÓN
Registro de Contenedores	- Deberá brindar un componente de registro centralizado para almacenar, administrar y distribuir imágenes de contenedores	Obligatorio
	- El componente de registro centralizado deberá tener compatibilidad con múltiples formatos de imagen, incluidos Docker, OCI y Helm	Obligatorio
	- El componente de registro centralizado deberá proporcionar almacenamiento y transferencia segura de imágenes	Obligatorio
	- El componente de registro centralizado deberá proporcionar control de acceso basado en roles (RBAC)	Obligatorio
	- El componente de registro centralizado deberá proporcionar auditoría y permitirá rastrear quién ha accedido a las imágenes y qué ha hecho con ellas	Obligatorio
	- El componente de registro centralizado deberá proporcionar escalabilidad y alta disponibilidad	Obligatorio
Registro de Artefactos	- Gestión Centralizada de Artefactos: Permite almacenar, organizar y gestionar artefactos de software en un repositorio centralizado. Estos artefactos pueden incluir librerías, paquetes, archivos binarios, entre otros	Obligatorio
	- Soporte para Múltiples Formatos de Paquetes: Son compatibles con una amplia variedad de formatos de paquetes, como Maven, npm, Docker, PyPI, NuGet, entre otros, facilitando la gestión de artefactos en diferentes lenguajes y plataformas	Obligatorio
	- Control de Versiones: Ofrece funcionalidades para gestionar las diferentes versiones de los artefactos, permitiendo a los usuarios almacenar y acceder a versiones específicas según sea necesario	Obligatorio
	- Seguridad y Control de Acceso: Implementa mecanismos de autenticación y autorización	Obligatorio



HERRAMIENTA	CARACTERÍSTICAS	PRIORIZACIÓN
	para controlar quién puede acceder, modificar o publicar artefactos, asegurando la integridad y seguridad de los mismos	
Gestor de automatización de la construcción del software, pipelines de integración y entrega continua (CI/CD)	- Multiprocesos: permite manejar múltiples trabajos y flujos de trabajo de forma simultánea	Obligatorio
	- Control de compilación: proporciona un control completo sobre el proceso de compilación, ofreciendo una amplia gama de complementos y configuraciones personalizables	Obligatorio
	- Depuración: configuración altamente personalizable	Obligatorio
	- Cifrado: ofrece opciones para garantizar la seguridad de sus pipelines, incluyendo el cifrado de datos y la autenticación	Obligatorio
	- Interfaz: contar con una interfaz de usuario basada en web	Obligatorio
Gestor de pruebas de performance	- Soporte de lenguaje de programación: permite crear scripts de prueba en diferentes lenguajes como Java y JavaScript	Obligatorio
	- Compatibilidad con navegador: permite probar el sitio web en diferentes navegadores como Google Chrome, Mozilla Firefox, Microsoft Edge, Safari, Internet Explorer (IE), etc	Obligatorio
	- Escalabilidad: las pruebas automatizadas pueden escalarse fácilmente para cubrir una amplia gama de casos de prueba, escenarios e interacciones de usuarios	Obligatorio
	- Pruebas paralelas: permite la ejecución de pruebas paralelas, lo que permite ejecutar varias pruebas simultáneamente	Obligatorio
	- Documentación e informes: proporciona registros e informes detallados de ejecución de pruebas	Obligatorio





HERRAMIENTA	CARACTERÍSTICAS	PRIORIZACIÓN
	- Permite integrar en pipelines de CI/CD para automatizar las pruebas de cada cambio de código fuente	Obligatorio
Gestor de análisis estático de código fuente	- Búsqueda de vulnerabilidades en el código fuente	Obligatorio
	- Análisis de las vulnerabilidades del código fuente en base a OWASP top 10 y CWE 25	Obligatorio
	- Soporte al lenguaje de programación JAVA, Javascript, .NET, entre otros	Obligatorio
	- Revisión automática con análisis estático del código fuente para detectar problemas que afectan la calidad del código	Obligatorio
	- Proporcionar informes con información de la calidad del código de los microservicios utilizando métricas y gráficos de prueba de calidad. Debe incluir datos sobre código duplicado, estándares de codificación, pruebas unitarias, cobertura de código, complejidad de código, errores potenciales, comentarios, diseño y arquitectura	Obligatorio
	- Integración con las herramientas de DevOps	Obligatorio
	- Las principales métricas para considerar son: <ul style="list-style-type: none"> • Duplicados Indica el número de bloques de líneas de código fuente duplicados. • Evidencias Son los fragmentos de código que detecta que incumplen con alguna de las reglas establecidas. • Mantenibilidad Se refiere al recuento total de problemas de Code Smell. • Umbral de calidad Define los requisitos del código antes de ser lanzado a producción, como, por ejemplo, que no debe haber evidencias bloqueantes o la cobertura de código sobre el código nuevo. • Pruebas 	Obligatorio



HERRAMIENTA	CARACTERÍSTICAS	PRIORIZACIÓN
	- Permite comprobar el correcto funcionamiento de una unidad de código y de su integración	Obligatorio
	- Permite integrar en pipelines de CI/CD para automatizar las pruebas de cada cambio de código fuente.	Obligatorio
Herramienta de escaneo de vulnerabilidades en contenedores	- Proporciona escaneo y corrección de vulnerabilidades para imágenes de contenedores, configuraciones de Kubernetes y aplicaciones en ejecución	Obligatorio
	- Utiliza aprendizaje automático y análisis de comportamiento para detectar comportamientos anómalos en clústeres y aplicaciones de Kubernetes. Cuando se detecta una amenaza, puede tomar medidas automáticamente para mitigar la amenaza, como aislar la aplicación afectada o revertir la configuración afectada	Obligatorio
	- Permite evaluar el riesgo del entorno de Kubernetes en función de factores como la cantidad de vulnerabilidades, la gravedad de esas vulnerabilidades y la probabilidad de explotación	Obligatorio
	- Debe ser basado en tecnologías de código abierto, como Kubernetes y Prometheus.	Obligatorio
Herramienta para automatización de operaciones TI	- Permitirá su habilitación sin instalar ningún agente (agentless) en los nodos a automatizar	Obligatorio
	- Proporcionar capacidad para integrarse con otras herramientas a través de REST-API	Obligatorio
	- Capaz de hacer la automatización para múltiples sistemas operativos (al menos Linux, MS Windows, UNIX)	Obligatorio
	- Capaz de hacer automatización a servidores físicos	Obligatorio
	- Capaz de hacer la automatización hacia la infraestructura virtual (al menos vSphere, Hyper-V, KVM)	Obligatorio



HERRAMIENTA	CARACTERÍSTICAS	PRIORIZACIÓN
	- Capaz de hacer automatización hacia dispositivos de red físicos (switches, firewalls, routers, load balancers, etc.) de distintos fabricantes (Cisco, F5, Checkpoint, Fortinet, etc.)	Obligatorio
	- Debe contar con una consola de administración centralizada basada en GUI para administrar múltiples dispositivos	Obligatorio
	- Proporcionar control de acceso basado en roles para administrar el acceso y el privilegio de la automatización	Obligatorio
	- Proporcionar la capacidad de entregar funcionalidad de autoservicio para la ejecución de trabajos	Obligatorio
	- Proporcionar CLI (línea de comando) para el uso avanzado de la herramienta de automatización	Obligatorio
	- Proporcionar funcionalidades para implementar Infraestructura como código (IaC)	Obligatorio
	- Proporcionar la capacidad de ser auditado	Obligatorio
	- Capacidad para crear formularios de IU personalizados para variables de entrada al comenzar un trabajo	Deseable
	- Capacidad de ejecutar comandos remotos	Obligatorio
	- Proporcionar la capacidad de rastrear los trabajos que se han ejecutado, recopilar información sobre el éxito y el estado de error para los trabajos	Obligatorio
	- Proporcionar capacidad para definir el flujo de trabajo para múltiples trabajos de automatización	Obligatorio

Las herramientas de desarrollo y DEVSECOPS ofertadas deberán ser instaladas y configuradas sobre la plataforma de orquestación de contenedores ofertada en el Anexo 02.

El contratista deberá brindar licenciamiento o suscripción de Las herramientas de desarrollo y DEVSECOPS por el periodo de 03 años, contabilizados a partir del día siguiente de la entrega de las licencias o suscripciones. A continuación, se describen las cantidades que se requieren licenciar o suscribir por cada herramienta:

- Gestor de Código Fuente – 80 usuarios nombrados
- Registro de Contenedores – 30 usuarios nombrados
- Repositorio de Artefactos – 30 usuarios nombrados
- Gestor de automatización de la construcción del software, pipelines de integración y entrega continua (CI/CD) – 30 usuarios nombrados
- Gestor de Pruebas de Performance - 30 usuarios nombrados
- Gestor de análisis estático de código fuente – 80 usuarios nombrados
- Escaneo de vulnerabilidades de contenedores – 30 usuarios nombrados
- Herramienta de automatización de operaciones TI – 30 usuarios nombrados y gestión de hasta 100 endpoints.



ANEXO 04

ESPECIFICACIONES TÉCNICAS DE LAS HERRAMIENTAS DE LA ARQUITECTURA DESACOPLADA PARA LOS AMBIENTES DE DESARROLLO, INTEGRACIÓN Y PRUEBAS DEL SIIRC

La arquitectura desacoplada del SIIRC está conformada por las siguientes capas de arquitectura:

- Capa de Interfaz / Bloque de funcionalidad
- Capa de Coreografías de Negocio o Procesos
- Capa de Reglas de Negocio
- Capa de Actividades Robóticas
- Capa de APIs
- Capa de Eventos
- Capa de Microservicios
- Capa de Documentos Electrónicos
- Capa de Componentes

La implementación del SIIRC se va a realizar utilizando la tecnología JAVA, en consecuencia, las herramientas de la Arquitectura Desacoplada deben soportar dicha tecnología.

En la presente contratación se adquirirán las herramientas de Software API Manager, gestión de identidades y control de accesos, streaming de datos en tiempo real. Las herramientas serán desplegadas en los ambientes de desarrollo, integración y pruebas. Deberán tener las siguientes especificaciones:

SOFTWARE API MANAGER

REQUERIMIENTOS	PRIORIZACIÓN
El software permite publicar APIs utilizando módulo de publicación. UI con portal	Obligatorio
El software permite el control de accesos basado en roles, para separación de desarrolladores y publicadores de los APIs	Obligatorio
El software permite realizar procesos de promoción de cambios. Generación de documentación (Swagger / I/O Docs).	Obligatorio
El software permite realizar función QoS – API Gateway que actúe como proxy para servicios backend y realice funciones de calidad de servicio con seguridad, políticas de uso de los APIs y analíticas.	Obligatorio
El software permite el monitoreo y reporte de uso de los APIs.	Obligatorio

REQUERIMIENTOS	PRIORIZACIÓN
El software brinda seguridad a las APIs, soporte de especificaciones de OAuth en caso de credenciales de clientes, claves, OpenID Connect, OAuth2, Basic Authentication, APIKey, MutualTLS, (SAML 2.0 opcional), etc. que permitirá el uso de los APIs por diferentes tipos de aplicaciones de manera segura.	Obligatorio
Permite el manejo de esquemas SSO.	Obligatorio
El software soporta manejo de versiones de API.	Obligatorio
El software puede realizar notificaciones para casos que no se cumplan con los SLA establecidos o integrarse a un software de monitoreo externo que permita implementar las notificaciones.	Obligatorio
El software tiene la capacidad de generar reportes con estadísticas de uso incluyendo como mínimo sistemas de monitorización y análisis desde la perspectiva del consumidor: timing, estatus, disponibilidad, consumo de APIs, etc.	Obligatorio
El software tiene capacidad para automatizar el despliegue al API Manager	Obligatorio
El software tiene capacidad de integrarse con herramientas de Integración Continua	Obligatorio
El software trabaja con distintas convenciones RESTful	Obligatorio
El software puede realizar la transformación de los mensajes obtenidos de los backends mediante mediación.	Obligatorio
El software brinda información completa de las APIs registradas, las cuales pueden ser descargadas.	Obligatorio
El software permite el manejo de ciclo de vida de las APIs	Obligatorio
El software tiene un flujo de publicación de APIs	Obligatorio
El software puede orquestar múltiples llamadas de backends	Obligatorio
El software permite invocar servicios REST, SOAP	Obligatorio
El software permite la actualización de metadatos en cada API.	Obligatorio
El software tiene un flujo de aprobación para el registro de aplicaciones o para el registro a suscripciones a productos de APIs.	Obligatorio
El software alerta cuando se incumplió una regla establecida	Obligatorio



REQUERIMIENTOS	PRIORIZACIÓN
El software tiene herramientas de logs y trace en tiempo de ejecución	Obligatorio
El software permite realizar un monitoreo del estatus actual de cada API desplegada	Obligatorio
El software puede integrarse a herramientas de monitoreo	Obligatorio
El software debe ser instalado de forma on-premise en el centro de datos del RENIEC.	Obligatorio
El software debe desplegarse sobre una plataforma de orquestación de contenedores.	Obligatorio
Gobierno	
El software debe considerar herramientas para la gestión de versionamiento de APIs.	Obligatorio
El software debe estar preparada para que una API se promueva hacia ambientes de producción y en cada ambiente tener accesos/roles.	Obligatorio
El software debe permitir configurar cantidad de llamadas máxima configuradas a través de planes, debe poseer diversos planes y debe soportar personalizaciones.	Obligatorio
Manager	
El software debe permitir desarrollar políticas personalizadas. Debe proveer un lenguaje de programación o mecanismos para el desarrollo de estas políticas personalizadas.	Obligatorio
La autenticación para ingresar al portal de Desarrollador debe soportar la integración con un LDAP, por ejemplo, el MS Active Directory.	Obligatorio
Portal de desarrollador	
El software debe proveer un portal de desarrollador que sea responsive.	Obligatorio
El software debe mostrar de manera amigable todo lo que documentas en el API mediante Swagger o similar, por ejemplo, si se coloca descripción de los campos de request y response, entonces el portal te muestra todo esto, pero en tablas y con colores.	Obligatorio



REQUERIMIENTOS	PRIORIZACIÓN
Seguridad	
El software debe soportar diferentes mecanismos de autenticación, es decir quiero que para un grupo de consumidores autentique por client-id + client-secret, pero para otros con OAUTH, por ejemplo.	Obligatorio
Las APIs deben incluir algunas de las siguientes formas de autenticación: <ul style="list-style-type: none"> • Vía token de JWT • Vía OAUTH • Otros mecanismos de seguridad soportados, por ejemplo, JWT 	Obligatorio
Gateway	
El software debe soportar tecnología open source para desarrollar el API Gateway	Deseable
Análítica de los datos	
El software debe tener módulo de análisis de la información de los datos que recolecta la solución	Obligatorio
La solución debe proveer los siguientes reportes de análisis en tiempo real: <ul style="list-style-type: none"> • Uso general de cada API hasta el nivel del método • Lista de aplicaciones • Tendencias de las APIs con uso máximo • Uso específico para cada aplicación en la API hasta el nivel del método 	Obligatorio
Diseño de APIs	
El software debe permitir usar los estándares o algunas de las siguientes herramientas de diseño: Open API, Swagger, RAML, BluePrint, etc.	Obligatorio

El contratista deberá brindar licenciamiento o suscripción del software API MANAGER ofertado por el periodo de 03 años, contabilizados a partir del día siguiente de la entrega de las licencias o suscripciones. A continuación, se describen las cantidades que se requieren licenciar o suscribir por cada ambiente:

- Ambiente de Desarrollo: 5,000,000 API call por mes.
- Ambiente de Integración: 4,000,000 API call por mes.
- Ambiente de Pruebas: 3,000,000 API call por mes.

Considerar que dentro del modelo de suscripción por API Calls se requiere flexibilidad para poder crecer en recursos de hardware asignados a cualquiera de los componentes de las instancias de API Management sin que esto represente un costo adicional para la Entidad.

El ambiente de Integración y Testing debe contar con un esquema de alta disponibilidad de al menos dos (02) replicas por contenedor/pod por cada componente.

SOFTWARE DE AUTENTICACIÓN PARA LA GESTIÓN DE IDENTIDADES Y CONTROL DE ACCESOS

REQUERIMIENTOS	PRIORIZACIÓN
<p>El software soporta los protocolos:</p> <ul style="list-style-type: none"> • OpenID Connect • OAuth 2.0 • SAML 2.0 • LDAP • Kerberos • Debe permitir el inicio de sesión usando redes sociales (Google, GitHub, Facebook, Twitter y otras redes sociales). 	Obligatorio
<p>El software permite la integración:</p> <ul style="list-style-type: none"> • Integración con aplicaciones Java mediante adaptadores. • Integración con aplicaciones externas mediante protocolos estándar como OIDC y SAML. 	Obligatorio
<p>El software proporciona seguridad:</p> <ul style="list-style-type: none"> • Permite la gestión de políticas de seguridad y acceso. • Soporte para autenticación multifactor (MFA). • Configuración de tokens JWT (JSON Web Tokens) para la seguridad de las sesiones. 	Obligatorio
<p>El software permite la administración:</p> <ul style="list-style-type: none"> • Interfaz de administración basada en web. • API REST para la automatización y gestión programática. 	Obligatorio
<p>El software permite la personalización:</p> <ul style="list-style-type: none"> • Posibilidad de personalización de temas y flujos de autenticación mediante extensiones y scripts. 	Obligatorio
El software debe ser instalado de forma on-premise en el centro de datos del RENIEC	Obligatorio



REQUERIMIENTOS	PRIORIZACIÓN
El software debe desplegarse sobre una plataforma de orquestación de contenedores.	Obligatorio

El contratista deberá brindar licenciamiento o suscripción del software de AUTENTICACIÓN PARA LA GESTIÓN DE IDENTIDADES Y CONTROL DE ACCESOS ofertado por el periodo de 03 años, contabilizados a partir del día siguiente de la entrega de las licencias o suscripciones. A continuación, se describen las cantidades que se requieren licenciar o suscribir por cada ambiente:

Ambiente	Cantidad de Cores
Desarrollo	4 cores físicos o 8 vcpus
Integración	4 cores físicos o 8 vcpus
Pruebas	8 cores físicos o 16 vcpus



SOFTWARE DE STREAMING DE DATOS EN TIEMPO REAL



REQUERIMIENTOS	PRIORIZACIÓN
El software debe soportar arquitectura basada en eventos, así como el diseño de aplicaciones y servicios que respondan en tiempo real a información basada en enviar y recibir notificaciones de cambios individuales en el sistema.	Obligatorio
El software debe soportar arquitectura de componentes distribuidos, bus de datos (Intermediario) y comunicación asíncrona que permita publicar información de distintas fuentes y ponerla a disposición de otras aplicaciones que necesiten dicha información.	Obligatorio
El software debe soportar la centralización de distintas fuentes de información, almacenar dicha información con tolerancia a fallos y alta disponibilidad.	Obligatorio
El software debe soportar escalamiento horizontal y absorber picos de carga que se puedan generar durante la centralización de las fuentes de información.	Deseable
El software debe soportar la creación de aplicaciones de transmisión de eventos con Apache Kafka utilizando diversos clientes nativos, como Java y muchos más lenguajes con enlaces de librdkafka.	Obligatorio



REQUERIMIENTOS	PRIORIZACIÓN
El software debe permitir integrar aplicaciones en tiempo real a través de una plataforma de Streaming de Eventos.	Obligatorio
El software debe permitir construir aplicaciones productoras que publiquen eventos, así como aplicaciones consumidoras que reaccionan a dichos eventos.	Obligatorio
El software debe permitir construir eventos que se almacenan de manera persistente de tal manera que, ante un problema en las aplicaciones consumidoras, estas pueden volver a leer los mensajes de nuevo.	Obligatorio
El software debe ser una distribución de Apache Kafka.	Obligatorio
El software debe permitir monitorizar la salud de los Clústers de Apache Kafka, gestionar Topics, monitorizar data streams, etc.	Obligatorio
El software debe soportar CLI (command line) o GUI que permita efectuar operaciones como gestión de credenciales, gestión de roles y accesos, etc.	Obligatorio
El software debe soportar conectores que se pueden utilizar tanto para cargar información en Apache Kafka (sources) como para enviar información procesada en Apache Kafka a sistemas terceros.	Obligatorio
El software debe permitir que los mensajes una vez recibidos y persistidos no puedan ser eliminados de manera independiente, sino que persisten en función del tiempo especificado en la política de retención.	Obligatorio
El software debe permitir que los consumidores estén constantemente escuchando mensajes nuevos.	Obligatorio
El software debe garantizar el orden de entrega de los mensajes.	Obligatorio
El software debe permitir mantener de manera redundante diferentes particiones de cada mensaje.	Obligatorio
El software debe permitir que, ante un fallo en esa partición, los restantes elementos del clúster puedan continuar dando servicio usando la copia que tienen de las particiones.	Deseable
El software debe permitir a los consumidores se puedan agrupar en grupos de consumidores y agregar o eliminar consumidores de un grupo.	Obligatorio





REQUERIMIENTOS	PRIORIZACIÓN
El software debe permitir una tecnología elástica, escalable y permitir streaming storage.	Obligatorio
El software debe permitir guardar datos históricos todo el tiempo que sea necesario (configurable) y reproducir estos datos históricos.	Obligatorio
El software debe permitir procesar, analizar los flujos y tablas de datos en tiempo real, 24 horas al día y 7 días a la semana.	Obligatorio
El software debe proporcionar un conector JMS Client como soporte para aplicaciones de Java Message Service (JMS) heredadas que consumen y producen directamente desde Kafka.	Obligatorio
El software debe proporcionar seguridad de nivel empresarial RBAC (Rol Basado en Control de Accesos), autorización granular de acceso por parte de usuarios/grupos para evitar violaciones de seguridad, observabilidad de las acciones de los usuarios relacionadas con la seguridad para simplificar los análisis y análisis forenses, Cifrado incorporado de información confidencial (por ejemplo, contraseñas y otras credenciales).	Obligatorio
El software debe contar con la capacidad de procesamiento en tiempo real	Obligatorio
El software debe ser instalado de forma on-premise en el centro de datos del RENIEC.	Obligatorio
El software debe desplegarse sobre una plataforma de orquestación de contenedores.	Obligatorio



El contratista deberá brindar licenciamiento o suscripción del software de STREAMING DE DATOS EN TIEMPO REAL ofertado por el periodo de 03 años, contabilizados a partir del día siguiente de la entrega de las licencias o suscripciones. A continuación, se describen las cantidades que se requieren licenciar o suscribir por cada ambiente:

Ambiente	Kafka brokers (cantidad/cores)	Kafka Connectors	Zookeepers	Flujos de Streams	Total de Cores
Desarrollo	3 unidades / 1 core (c/u)	1 unidad / 1 core (c/u)	3 unidades / 1 core (c/u)	1 unidad / 1 core	8
Integración	3 unidades / 1 core (c/u)	2 unidades / 0.5 core (c/u)	3 unidades / 1 core (c/u)	2 unidades / 1 core	9
Pruebas	3 unidades / 1 core (c/u)	2 unidades / 0.5 core (c/u)	3 unidades / 1 core (c/u)	2 unidades / 1 core	9

El contratista podrá considerar los componentes adicionales que requiera e incluirlos en su modelo de licenciamiento o suscripción para el correcto funcionamiento de la plataforma de streaming de eventos en tiempo real.

Considerar que los componentes que tienen cantidades superiores a uno (01) deben ser desplegados en nodos de trabajo independientes dentro del clúster de contenedores.



ANEXO 05
ESPECIFICACIONES TECNICAS DE LA BASE DE DATOS PARA LA PLATAFORMA
DE ORQUESTACIÓN DE CONTENEDORES PARA LOS AMBIENTES DE
DESARROLLO, INTEGRACIÓN Y PRUEBAS DEL SIIRC

El RENIEC cuenta con productos de software Oracle, los cuales a la fecha cuentan con una estandarización para el servicio de soporte técnico.

Resolución de la Oficina de Administración y Finanzas Nº 000439-2024/OAF/RENIEC

<https://www.gob.pe/institucion/reniec/normas-legales/6161572-000439-2024-oaf-reniec>

La base de datos solicitada para implementar la plataforma de orquestación de contenedores para los ambientes de desarrollo, integración y pruebas debe tener las siguientes especificaciones:

SERVIDOR DE BASE DE DATOS

CARACTERISTICAS	PRIORIZACIÓN
Cantidad: 01 Equipo	Obligatorio
Servidor Rackeable	Obligatorio
Un (01) procesador por nodo con fecha de lanzamiento a partir del Q1 del 2024 El procesador debe tener (16 cores, 2.8 GHz, 37.5 MB de cache L3, 195 Watts) como mínimo	Obligatorio
16 módulos de 32 GB de 5600 MHz tipo RDIMM, de tecnología ECC	Obligatorio
Mínimo 04 puertos Ethernet de 10/25Gb SFP+ (LAN) incluyendo 04 Transceiver de 10Gb Mínimo 02 puertos Ethernet RJ45 de 1Gb Mínimo 02 puertos Fibre Channel 32 Gb 2 puertos PCIe V2	Obligatorio
Dos (02) discos de SSD 3,84 TB, lecturas intensivas, SATA 6 Gb de intercambio en caliente	Obligatorio
Dos (02) fuentes de poder tipo Hot Swap redundantes y de 800W (220V) como mínimo	Obligatorio
Todos los componentes, partes y/o piezas, cables y accesorios, deben ser originales y mínimamente fabricados el año 2024	Obligatorio
- Soporte de TPM 2.0. - El servidor debe cumplir con el NIST SP 800-147B.	Obligatorio



CARACTERÍSTICAS	PRIORIZACIÓN
<ul style="list-style-type: none"> - Sistema de arranque (boot) seguro, que garantice que solo se cargue software inmutable y firmado durante el tiempo de arranque, evitando que se cargue código malicioso y ayudando a prevenir ataques como la instalación de rootkits. - Protección contra actualizaciones de firmware no autorizadas y corrupción, restaurando el firmware a un estado integral y monitoreo del firmware en busca de posibles compromisos de ataques cibernéticos. - Contar con procesos de firma de firmware que cumplen con los requisitos de FIPS y NIST. 	
El servidor debe contar con Sistema Operativo Linux con soporte Empresarial, así como con Linux KVM	Obligatorio
El servidor debe permitir crear máquinas virtuales que permitan licenciar solo los core activos para los servicios dedicados de base de datos. Optimizando los costos de licenciamiento.	Obligatorio
<p>El servidor debe de tener:</p> <p>Certificado de no perjudicar la salud y/o presentar un impacto negativo al medio ambiente EPEAT.</p> <p>Certificado de eficiencia de energía (Energy Star).</p>	Obligatorio
<p>Software de Administración que permita lo siguiente:</p> <ul style="list-style-type: none"> - La administración centralizada de todos los dispositivos desde una única interfaz - La gestión de inventarios y el seguimiento de activos de hardware - Actualizaciones de firmware de manera centralizada, asegurando que todos los dispositivos estén ejecutando las versiones más recientes y seguras - Programar actualizaciones fuera de horario para minimizar el impacto en las operaciones - Integración con otras herramientas de gestión y orquestación, mínimamente con las herramientas ofertadas - Aplicación para la administración remota, permitiendo a los administradores supervisar y gestionar la infraestructura desde cualquier lugar - Alertas en tiempo real, vistas del estado del sistema y capacidades de resolución de problemas - Arquitectura sin agentes externos - Proporcionar datos para mejorar la eficiencia operativa de la infraestructura 	Obligatorio





CARACTERÍSTICAS	PRIORIZACIÓN
<ul style="list-style-type: none">- Informes detallados y cuadros de mando (dashboards) personalizables que permiten a los administradores obtener una visión completa del rendimiento y la salud de la infraestructura	
<ul style="list-style-type: none">- La garantía y soporte debe ser por tres (03) años y estar disponible las 24 horas de los 07 días de la semana, incluido feriados, durante el período de 03 años con tiempo de respuesta de 04 horas por parte del contratista y del fabricante- RMA (Return Merchandise Authorization), es decir autorización de devolución de mercancía: El contratista como parte del soporte y garantía ofertada, debe incluir el suministro de equipos en calidad de RMA por el periodo de tres (03) años, para el reemplazo respectivo de los mismos, cuando el equipo quede en estado inoperativo y sin diagnóstico por más de 72 horas, se debe reemplazar el equipo por parte del contratista y/o fabricante- El plazo de reemplazo del hardware será de 15 días calendarios como máximo- El equipamiento debe contar con Soporte técnico del fabricante para hardware y/o software a través de una línea gratuita 0-800- Deberá permitir el registro de solicitudes de soporte a través de un portal web del contratista y/o fabricante para el seguimiento y control de los incidentes y/o requerimientos- El soporte y la garantía podrá ser atendida de manera remota y/o presencial en coordinación con el RENIEC- El contratista deberá presentar una carta del fabricante confirmando lo solicitado, esta carta debe ser presentada al entregar el equipamiento, asimismo, la carta deberá considerar la Disponibilidad de Upgrade, parches del software para el equipo- La garantía y soporte iniciará a partir del día siguiente de la entrega de las licencias.- La carta de garantía emitida por el fabricante o sucursal del fabricante por tres (03) años en partes, mano de obra y on site para todas sus partes y componentes por defectos de fábrica, contados a partir del día siguiente de instalación y configuración.	Obligatorio



SOFTWARE DE BASE DE DATOS

REQUERIMIENTOS	PRIORIZACIÓN
<p>Software de Base de Datos Oracle Database Enterprise Edition Perpetual (EE) última versión disponible.</p> <p>Adicionalmente, debe considerar los siguientes componentes:</p> <ul style="list-style-type: none">- ORACLE PARTITIONING	Obligatorio



El software incluye: Servicios de implementación, soporte y garantía del fabricante de tres (03) años, que comienza a partir del día siguiente de la entrega de la licencia.	Obligatorio
Licencias del software de base de datos Oracle Database Enterprise Edition Perpetual para: - Ambiente de Desarrollo: 1 core. - Ambiente de Integración: 1 core. - Ambiente de Pruebas: 2 cores. Se debe incluir el respectivo soporte y mantenimiento de estas licencias por parte del proveedor.	Obligatorio
Las licencias serán implementadas en los ambientes de Desarrollo, Integración y Pruebas.	Obligatorio
Las licencias de deben contar con soporte y garantía del fabricante por un periodo de tres (03) años en modalidad 24x7, para todos los componentes del sistema ORACLE. El soporte y mantenimiento puede ser por canal telefónico o mediante canal web gestionado, brindado por el mismo fabricante y/o contratista.	Obligatorio
Durante el periodo de la garantía postventa debe incluir sin costo el privilegio de actualización a nuevas versiones del software.	Obligatorio
El fabricante de software de base de Datos debe contar con un portal web de atención 24x7, donde se pueda escalar y/o reportar problemas de software.	Obligatorio
El fabricante de software debe contar con un portal donde se puedan descargar actualizaciones, parches, recomendaciones de software.	Obligatorio
El contratista debe considerar dentro de su oferta la herramienta de virtualización y el Sistema Operativo Linux Enterprise. El virtualizador debe soportar la política de HARD PARTITIONING del fabricante de base de datos Oracle o equivalente.	Obligatorio
El Sistema Operativo y el Virtualizador deben estar certificados con la base de datos ORACLE.	Obligatorio



Etapas de instalación y configuración de la Base de Datos:

- El contratista deberá levantar información de las Base De Datos ORACLE del RENIEC de la infraestructura adquirida como parte del Producto 20: Equipamiento de Hardware y Software de Base para el SIIRC instalado y configurado. Con la finalidad de revisar

la configuración de la base de datos de producción para realizar la configuración de las bases de datos de desarrollo, integración y pruebas.

- El contratista deberá instalar y asignar las licencias en una VM con HARD PARTITIONING en el servidor de base de datos.
- El contratista brindara el virtualizador que permita HARD PARTITIONING y el Sistema Operativo Linux Empresarial donde se instalara la base de datos Oracle Enterprise Edition.
- El contratista deberá brindar la arquitectura recomendada de implementación a nivel de base de datos Oracle.
- Adicionalmente el contratista deberá configurar las bases de datos Oracle:
 - Base de datos de Pruebas con almacenamiento de 80 TB.
 - Base de datos de Integración con almacenamiento de 20 TB.
 - Base de datos de Desarrollo con almacenamiento de 20 TB.
- Estas bases de datos deben conectarse de forma directa y total con la plataforma de gestión de contenedores propuesta.
- El servicio de base de datos Oracle debe tener la funcionalidad de backup automático con retención máximo de 30 días.
- El servicio de base de datos Oracle debe de tener la funcionalidad activa de auditoría de accesos sobre la base de datos.
- Debe brindar soporte de bolsa de 240 horas anuales en modalidad 24x7 durante la vigencia de tres (03) años, el soporte debe incluir:
 - Atención a incidencias presentadas en las bases de datos.
 - Revisiones mensuales de 4 horas, del estado de las bases de datos y del backup, para lo cual debe de generar un informe técnico con recomendaciones.
 - El soporte debe incluir también aplicación de parches en las bases de datos
 - Soporte a incidencias presentadas en la copia de seguridad de la base de datos (rman).
 - El soporte debe incluir configuraciones en las bases de datos y en la copia de seguridad, aplicando mejores prácticas.

La solicitud de servicio se podrá realizar mediante los siguientes canales: telefónicamente o por correo electrónico. Se deberá proporcionar un primer nivel de atención, a través de una mesa de ayuda propia, para el soporte técnico de cualquiera de los productos de la plataforma de base de datos. El contratista deberá brindar los números de teléfono y direcciones de correo electrónico de contacto para el reporte de incidentes.

Para la prestación del servicio, se debe considerar el grado de severidad de los casos que se presentan:

- | |
|---|
| <ul style="list-style-type: none">• Severidad 1: Incidente de nivel crítico, inoperatividad total de la base de datos, o alto riesgo de que en cualquier momento quede inoperativa. Presencia en sitio de manera obligatoria.• Severidad 2: Incidente de nivel moderado, base de datos trabajando en modalidad degradada, o riesgo inminente de que en cualquier momento degrade su rendimiento.• Severidad 3: Incidente de nivel leve o requerimiento técnico. |
|---|



* Es posible que se pueda escalar un requerimiento hacia una severidad superior.

Se requiere que el servicio tenga un nivel de respuesta efectiva de acuerdo con la severidad:

Nivel de servicio	Tiempo de respuesta	Tiempo de solución
Severidad 1	30 minutos	04 horas
Severidad 2	2 horas	10 horas
Severidad 3	3 horas	15 horas

En caso de que el incidente vaya a tomar más tiempo, es necesario informar a RENIEC para analizar las acciones a realizar.

En caso se encuentre error desconocidos por la solución, se debe de abrir un caso con el fabricante para su pronta resolución. Es necesario hacer el seguimiento de dichos casos en coordinación con RENIEC.

