PLIEGO DE TÉRMINOS DE REFERENCIA PARA EL DESARROLLO DEL NUEVO SISTEMA DIGITAL DE INFORMACIÓN DE PRESTACIONES AL AMPARO DEL CMISS

1. Introducción

1.1 Antecedentes

El Convenio Multilateral Iberoamericano de Seguridad Social (CMISS) es un instrumento internacional creado para proteger los derechos de las personas trabajadoras migrantes y sus familias en el ámbito de las prestaciones económicas. Este convenio facilita la coordinación entre las legislaciones nacionales de los Estados Iberoamericanos en materia de pensiones, procurando la seguridad económica en situaciones de vejez, incapacidad o muerte. Este Convenio ha sido firmado por 16 países y está vigente en 13 de ellos, con el objetivo de continuar ampliando el número de Estados Parte. Para más información acerca del CMISS: https://oiss.org/convenio-multilateral/

El máximo órgano responsable de velar por la correcta implementación del CMISS es el Comité Técnico Administrativo del CMISS, formado por representantes de los Estados Parte del mismo. Este Comité ha acordado ya 10 formularios para pautar el intercambio de información entre Estados Parte relativa a la solicitud y tramitación de prestaciones al amparo del CMISS y podría acordar más en el futuro o modificar los actuales. Con el fin de agilizar ese proceso de intercambio de información entre Estados Parte, en el pasado se dispuso de un sistema de transferencia electrónica de información, que no pudo ser actualizado para cumplir con las necesidades de los Estados Parte. Por ello, en octubre de 2023, el Comité Técnico Administrativo del CMISS acordó iniciar el proceso de diseño de un nuevo sistema.

Asimismo, este Comité aprobó la propuesta de diseño del nuevo sistema que se anexa (Ver Anexo I) en el marco del cual se realiza este proceso de selección.

La Organización Iberoamericana de Seguridad Social (OISS), organismo internacional de carácter técnico constituido en 1954 para la promoción de la protección social en Iberoamérica ejerce como secretaría técnica del CMISS y será responsable del proceso de selección y contratación de esta consultoría, gracias al apoyo de la Agencia Española de Cooperación Internacional para el Desarrollo (AECID). Así, para continuar avanzando en materia de coordinación y adaptándose a los estándares tecnológicos actuales, el "Nuevo Sistema Digital de Información de Prestaciones al Amparo del CMISS" (en adelante, nueva aplicación), incorporará tecnologías modernas y mejores prácticas en el ámbito de la seguridad social para facilitar el intercambio de información entre los Estados Parte, basada en los formularios aprobados (Ver en https://oiss.org/convenio-multilateral/formularios/).

1.2 Objetivo del Pliego

El presente pliego de términos de referencia tiene como objetivo definir las bases y condiciones para el proceso de selección abierto destinado a seleccionar un proveedor

para el desarrollo de la nueva aplicación. Este documento establece el marco de trabajo, los requisitos técnicos y funcionales, así como las condiciones contractuales necesarias para la ejecución del proyecto. La nueva aplicación procurará la eficiencia, seguridad y capacidad de respuesta en la gestión de prestaciones en el marco del CMISS, proporcionando una solución robusta y escalable que se adapte a las necesidades de los Estados Parte.

La contratación se realizará mediante la firma de un acuerdo de colaboración y la aceptación de las condiciones técnicas y económicas remitidas por el proveedor seleccionado. Esta contratación en ningún caso supondrá una vinculación laboral con la OISS ni con los Estados Parte del CMISS o con ninguna de las entidades implicadas en la gestión e implementación del CMISS.

2. Contexto y Justificación

2.1 Situación Actual

Con el fin de facilitar la gestión de prestaciones al amparo del CMISS, se ha decidido desarrollar una aplicación que aproveche las últimas tecnologías y mejores prácticas. Esta iniciativa busca:

- **Actualización Tecnológica**: Adoptar tecnologías de vanguardia para mejorar el mantenimiento y actualización del sistema.
- **Seguridad Avanzada**: Incorporar medidas de seguridad modernas que cumplan con los estándares actuales, garantizando la protección de datos sensibles.
- **Experiencia del Usuario Mejorada**: Crear una interfaz de usuario intuitiva y moderna, optimizando la eficiencia operativa y la satisfacción del usuario.
- **Mayor Integración**: Facilitar la interoperabilidad con otros sistemas y plataformas mediante una mejor integración.

2.2 Justificación del Nuevo Sistema

El desarrollo de la nueva aplicación está justificado por la necesidad de mejorar y optimizar varios aspectos clave:

- **Eficiencia Operativa**: La nueva aplicación permitirá una gestión eficiente de las prestaciones, reduciendo los tiempos de procesamiento y mejorando la capacidad de respuesta.
- **Seguridad y Confidencialidad de Datos**: Implementará medidas de seguridad avanzadas para proteger los datos sensibles y cumplir con las normativas internacionales de protección de datos (especialmente las de la Unión Europea), garantizando la máxima seguridad y confidencialidad de la información.

- **Escalabilidad y Flexibilidad en Entorno Cloud**: Utilizando una arquitectura basada en tecnologías cloud, la nueva aplicación será escalable y flexible para adaptarse a las necesidades cambiantes.
- **Experiencia del Usuario**: Se desarrollará una interfaz de usuario moderna e intuitiva, mejorando la accesibilidad y usabilidad del sistema, asegurando agilidad, facilidad de uso y mantenimiento.
- **Sistema de Acceso Dual**: La nueva aplicación permitirá un doble sistema de acceso a la información:
    - **Entrada Manual (B2C)**: Los usuarios podrán ingresar datos manualmente a través de formularios publicados.
    - **Entrada Automática vía API (B2B)**: La nueva aplicación proporcionará APIs que permitirán la integración automática con los sistemas internos de los países miembros, facilitando el envío y recepción de información de manera automatizada.
- **Interoperabilidad**: La nueva aplicación permitirá una mejor integración con otros sistemas y plataformas, facilitando la interoperabilidad y el intercambio de datos.
- **Cumplimiento Normativo**: Asegurará el cumplimiento con las más altas regulaciones y normativas internacionales en materia de seguridad social y protección de datos.

La implementación de la nueva aplicación no solo mejorará la operatividad y eficiencia del CMISS, sino que también procurará la satisfacción de los usuarios y la protección adecuada de los datos. Este desarrollo es esencial para mantener la relevancia y efectividad del sistema de prestaciones en el contexto actual y futuro.

3. Requerimientos del Sistema

3.1 Requerimientos Funcionales

Descripción de los Módulos Funcionales de la Aplicación

La Nueva Aplicación se estructurará en varios módulos funcionales clave, cada uno con responsabilidades y características específicas para garantizar una gestión eficiente y segura de las prestaciones bajo el CMISS.

1. **Módulo de Gestión de Usuarios**:
    - **Registro y Administración de Usuarios**: Permite a los administradores delegados de cada país registrar nuevos usuarios y gestionar su ciclo de vida dentro de la plataforma, incluyendo activación, actualización, suspensión y eliminación de cuentas.

- **Asignación de Perfiles y Roles**: Facilita la asignación de roles específicos a los usuarios, definiendo claramente qué acciones están permitidas dentro de la plataforma según su posición y responsabilidades.
- **Ciclo de Vida de los Usuarios**: Gestión activa del ciclo de vida de los usuarios, abarcando desde su creación hasta su eventual baja del sistema, incluyendo la actualización periódica de permisos y la reasignación de roles.

2. **Módulo de Gestión de Formularios**:
   - **Parametrización y Flexibilidad**: Los administradores tomarán los campos incluidos en los formularios acordados por el Comité Técnico Administrativo, con la posibilidad de adaptarlos a futuros cambios en los requerimientos específicos de cada tipo de solicitud que el Comité Técnico Administrativo acuerde
   - **Relación con Roles de Usuario**: La gestión de formularios está ligada a los roles definidos en el módulo de Gestión de Usuarios, asegurando que las operaciones en los formularios se realicen siempre dentro del marco de seguridad y permisos adecuados.
   - **Gestión de Documentos Adjuntos**: Facilita la asociación y manejo de documentos adjuntos, permitiendo a los usuarios cargar, gestionar y adjuntar documentos necesarios a sus formularios.
   - **Configuración y Adaptación Continua**: Permite una actualización y configuración continua de los formularios para reflejar cambios legislativos, políticas específicas de países o mejoras en los procesos, siempre que estos cambios hayan sido aprobados por el Comité Técnico Administrativo.
3. **Módulo de Gestión de Validaciones**:
   - **Validación de Datos Estructurados**: Define y aplica reglas dinámicas para la validación de campos específicos en los formularios, asegurando la exactitud de los datos capturados.
   - **Validación de Datos No Estructurados**: Extiende la capacidad de validación a documentos y archivos adjuntos, verificando que cumplen con los requisitos de formato, tamaño y tipo.
   - **Validación de Seguridad de Documentos y Archivos Adjuntos**: Inspección de seguridad para verificar que los documentos y archivos adjuntos estén libres de virus o malware.
   - **Reglas de Validación Configurables**: Permite a los administradores configurar y actualizar las reglas de validación para adaptarse a cambios en los requerimientos legales o políticas internacionales.
   - **Retroalimentación y Corrección**: Ofrece retroalimentación inmediata sobre errores o inconsistencias, con sugerencias claras para su corrección.

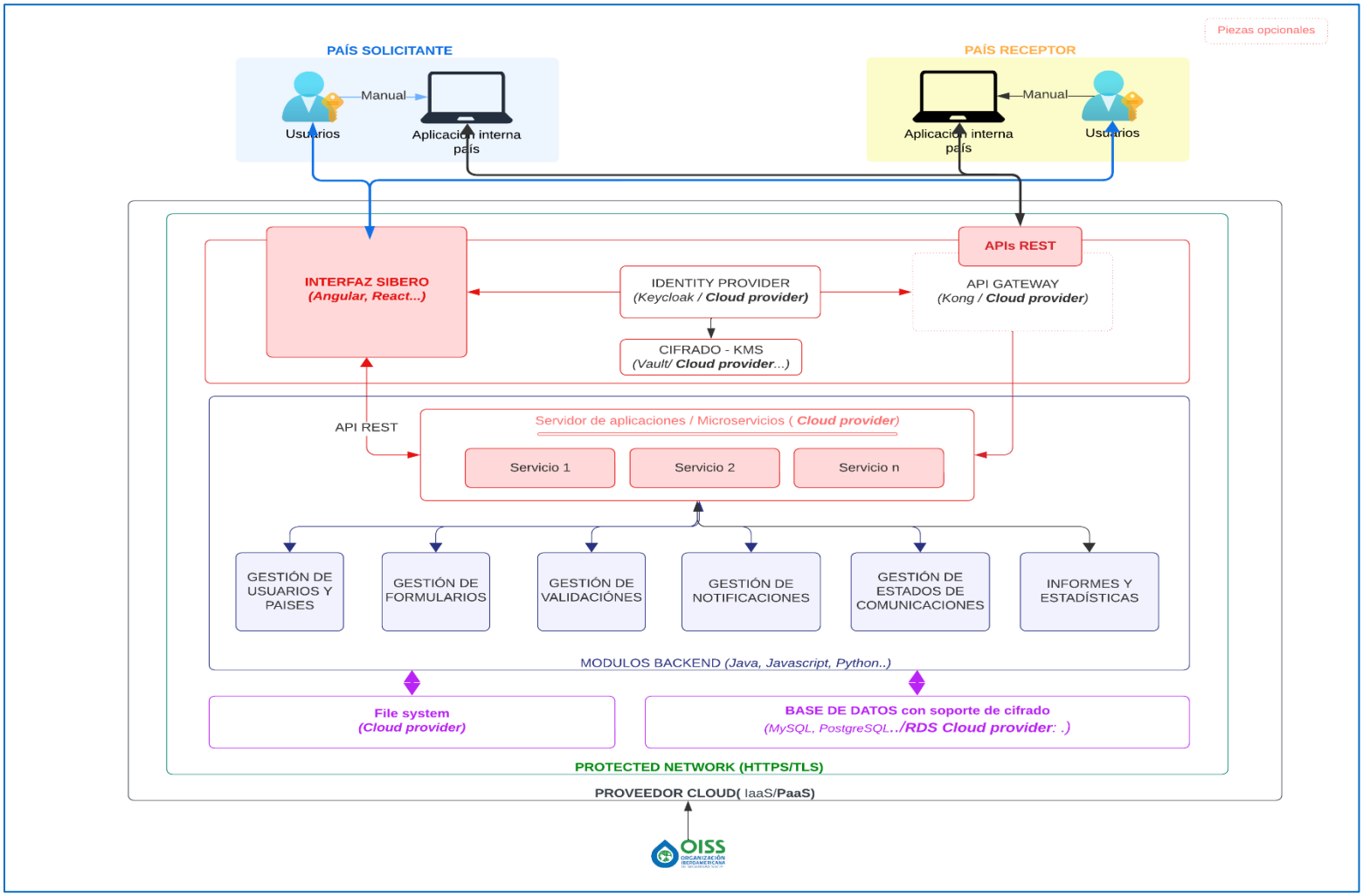
- **Registro y Auditoría**: Mantiene un historial completo de todas las validaciones realizadas, incluyendo errores detectados y acciones de corrección tomadas.

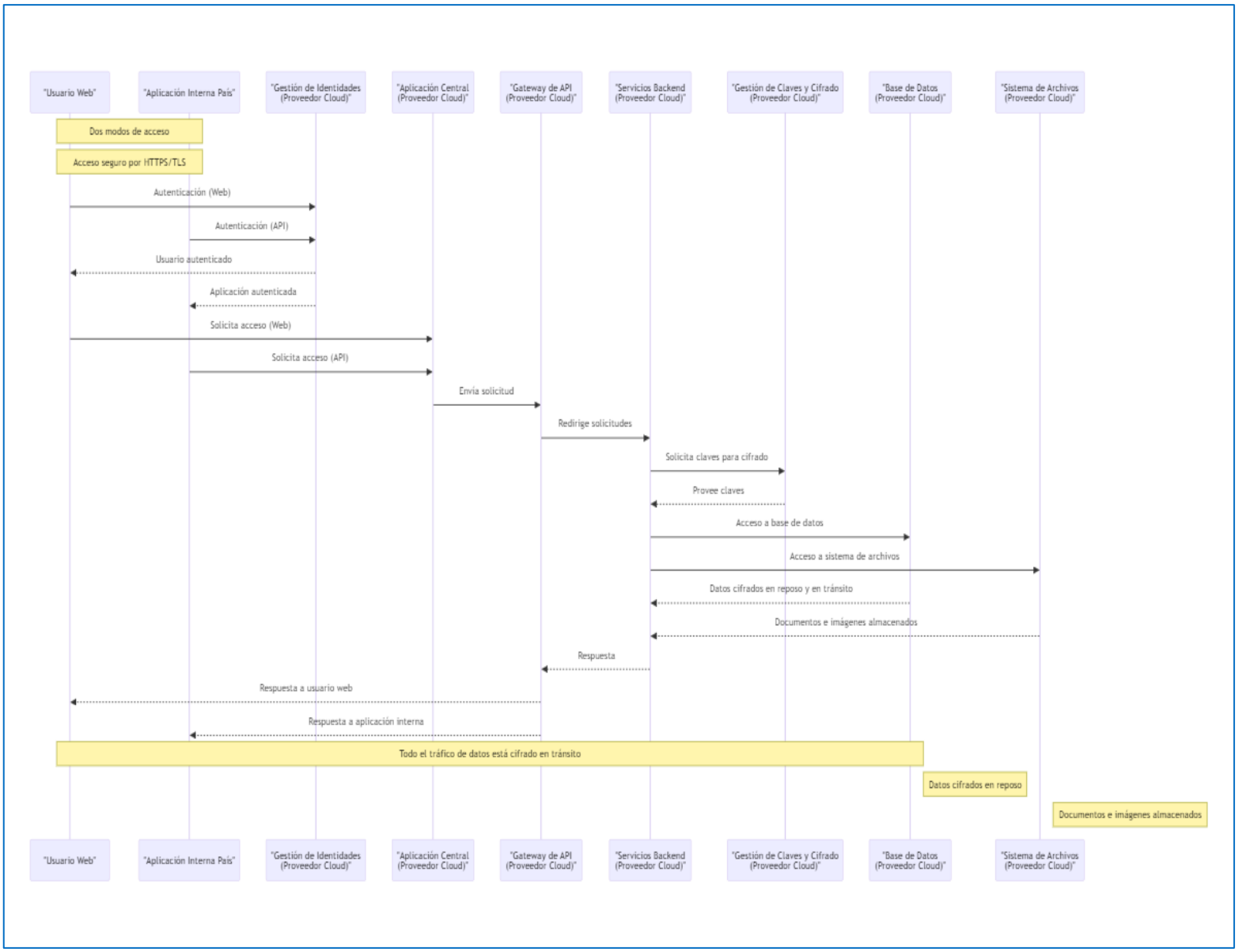
4. **Módulo de Gestión de Notificaciones**:
   - **Notificaciones Automatizadas**: Envía notificaciones automáticas a los usuarios basadas en eventos específicos dentro de la aplicación.
   - **Configuración de Notificaciones**: Los administradores pueden configurar y parametrizar el tipo, contenido y momento de las notificaciones.
   - **Personalización de Mensajes**: Permite personalizar los mensajes de notificación para incluir información relevante y específica.
   - **Diversos Canales de Comunicación**: Envía notificaciones a través de diversos canales, como correo electrónico y mensajes de texto.
   - **Seguimiento de Notificaciones**: Permite el seguimiento de las notificaciones enviadas, incluyendo detalles sobre la entrega y recepción.
5. **Módulo de Gestión de Estados**:
   - **Definición de Estados**: Administradores pueden definir una serie de estados a través de los cuales transitan las solicitudes, como "Pendiente de Validación", "En Revisión", "Aprobada", "Rechazada".
   - **Transiciones y Reglas**: Establece reglas y transiciones entre estados, definiendo acciones necesarias para que una solicitud pase de un estado a otro.
   - **Asociación con Acciones y Roles**: Cada estado puede estar asociado con acciones específicas que diferentes roles de usuario pueden realizar.
   - **Integración con Notificaciones**: Integra con el sistema de Gestión de Notificaciones para enviar alertas automáticas cada vez que una solicitud cambia de estado.
   - **Auditoría y Seguimiento**: Proporciona capacidades de auditoría y seguimiento, permitiendo ver el historial completo de estados por los que ha pasado cada solicitud.
6. **Módulo de Gestión de Informes**:
   - **Generación de Informes**: Permite la creación de informes dinámicos que reflejan distintos aspectos de la gestión de la plataforma.
   - **Desagregación de Datos**: Ofrece la capacidad de desglosar la información según varios criterios, como tipo de solicitud, país y período de tiempo.
   - **Exportación de Datos**: Permite la exportación de datos e informes en diferentes formatos para su análisis o presentación externa.
   - **Protección de la Información Personal**: Asegura que toda la información personal esté disociada o protegida, en línea con las regulaciones de protección de datos.
   - **Asociación con Roles y Permisos**: Control estricto del acceso a los informes y datos estadísticos, asignado según roles y permisos que acordará el Comité Técnico Administrativo del CMISS.

- **Visualización e Interpretación**: Incluye herramientas de visualización para facilitar la interpretación de los datos, como gráficos y tablas.

3.2 Requerimientos técnicos

La Nueva Aplicación deberá ser desarrollada e implementada con base en los siguientes requerimientos técnicos, tal y como queda reflejado en el diagrama a continuación, garantizando que se alinee con los estándares y mejores prácticas tecnológicas actuales.





1. **Entorno Cloud y Plataforma como Servicio (PaaS):**
    - **Despliegue en Cloud**: La aplicación deberá ser desplegada en un entorno cloud utilizando servicios de Plataforma como Servicio (PaaS). Preferentemente, se utilizarán productos y servicios propios del proveedor para evitar problemas de incompatibilidad y simplificar el mantenimiento y la adaptación futura. El desarrollo debe contemplar todo lo necesario para un eventual cambio de proveedor, incluyendo la posibilidad de una capa de abstracción entre la aplicación propiamente

dicha y los servicios cloud, si se considera conveniente. Asimismo, debe incluir un plan de salida para el caso de necesidad futura de cambio de proveedor.

- **Proveedor Cloud**: Se deberá seleccionar un proveedor cloud que ofrezca alta disponibilidad, escalabilidad automática y una suite integral de herramientas de desarrollo y gestión, así como estar en disposición de certificaciones de seguridad reconocidas internacionalmente (ISO 27001, ISO 27017, ISO 27018).

2. **Interfaz de Usuario y Acceso API:**

El acceso al nuevo sistema se ha diseñado para ser versátil y accesible, ofreciendo dos vías de entrada distintas que se adaptan a las necesidades de los usuarios finales y a las aplicaciones administrativas de los países miembros del convenio.

- **Interfaz Web**: La aplicación proporcionará una interfaz web intuitiva y segura. Esta interfaz debe permitir la autenticación de usuarios y acceso a funcionalidades relevantes de acuerdo con sus roles y permisos. La interfaz de usuario debe ser intuitiva, fácil de usar y accesible desde cualquier dispositivo con conexión a internet. Debe ser responsive y cumplir con los estándares de accesibilidad web.
- **APIs para Integración de Sistemas Internos**: Las aplicaciones internas de los países miembros deberán poder integrarse directamente con el nuevo sistema a través de APIs robustas y bien documentadas. Las APIs deben ofrecer un método programático para realizar operaciones, automatizar procesos y flujos de trabajo, e interactuar con el sistema central de forma eficiente.

El acceso deberá realizarse a través de un **API Gateway,** preferiblemente proporcionado por el proveedor cloud seleccionado, que garantice las siguientes funcionalidades:

- **Enrutamiento de Solicitudes**: El API Gateway actuará como un punto de entrada único para todas las solicitudes, dirigiéndolas a los servicios correspondientes y descomponiendo solicitudes complejas en múltiples solicitudes más simples.
- **Seguridad y Control de Acceso**: El API Gateway debe verificar las credenciales y tokens de acceso, asegurando que solo usuarios y aplicaciones autorizados puedan acceder a los servicios. Además, debe implementar políticas de seguridad como la limitación de tasa y la protección contra ataques comunes.
- **Manejo de APIs**: Debe gestionar diferentes versiones de las APIs y permitir la agregación de respuestas de múltiples servicios en una única

respuesta coherente. Todas las APIs deben cumplir con los lineamientos de OpenAPI.

- **Mejora del Rendimiento**: El API Gateway debe almacenar respuestas frecuentes en caché y distribuir las solicitudes entrantes entre instancias de servicios para optimizar el uso de recursos y mejorar el rendimiento.
- **SDKs y Documentación**: Deben ofrecerse kits de desarrollo de software (SDKs) y documentación detallada para facilitar la integración de las APIs.

3. **Arquitectura basada en servicios:**

   - Para la Nueva Aplicación, se ofrecen dos enfoques estructurales posibles: **Arquitectura de Microservicios** y **Arquitectura Monolítica con Servicios vía API**. Independientemente de la elección que el proveedor realice entre ambos posibles modelos, el diseño debe enfocarse en la creación de una arquitectura de servicios que permita una gestión descentralizada y la descomposición en servicios más pequeños.
   - **Gestión Descentralizada de Módulos**: Cada módulo funcional, descrito en la documentación funcional del sistema, debe ser capaz de operar de forma semi-independiente, facilitando una gestión y escalabilidad modular.
   - **Reutilización de Componentes**: Los componentes deben diseñarse para su reutilización en diferentes partes de la aplicación, ya sea a través de la interfaz web o como parte de las APIs para facilitar la integración con sistemas internos de los países.
   - **Integridad y Coherencia de Datos**: Es vital que ambos enfoques mantengan una integridad y coherencia de datos completa, garantizando que la información se maneje de manera uniforme a través de todas las plataformas y puntos de acceso.
   - **Seguridad y Escalabilidad**: Cada enfoque debe cumplir con altos estándares de seguridad (autenticación, cifrado, auditoría y monitorización…) y permitir una escalabilidad efectiva para acomodar un creciente número de usuarios y transacciones.

4. **Desarrollo de la Interfaz Web para el Acceso de los Países**

   La interfaz web del nuevo sistema constituye uno de los métodos de acceso para los países miembros, facilitando la interacción directa con el sistema a través de un portal web seguro y eficiente. Este acceso es fundamental para permitir la gestión y consulta de prestaciones de manera efectiva.

Requerimientos de Acceso y Usabilidad:

- **Diseño Responsive:** La interfaz debe ser totalmente funcional y óptima en una variedad de dispositivos, incluyendo ordenadores de escritorio, tablets y smartphones, asegurando una experiencia de usuario coherente y accesible desde cualquier dispositivo.
- **Navegación Intuitiva:** Se requiere que la estructura y navegación de la aplicación web sean claras y sencillas, permitiendo a los usuarios encontrar fácilmente la información necesaria y realizar las operaciones requeridas sin dificultades.
- **Accesibilidad:** La interfaz debe ser accesible para usuarios de diferentes regiones, ofreciendo soporte multilingüe y cumpliendo con las normativas internacionales de accesibilidad para asegurar que todos los usuarios, incluidos aquellos con discapacidades, puedan manejar eficientemente la aplicación.

Fundamentos Tecnológicos para el Desarrollo:

- **Uso de Frameworks Modernos:** Se deberá utilizar frameworks de desarrollo web modernos como React o Angular para la construcción de la interfaz, apoyando una arquitectura de componentes modulares y facilitando la mantenibilidad y escalabilidad del sistema.
- **Estrategias de Optimización Web:** Implementar técnicas avanzadas para optimizar la carga de la página, mejorando el rendimiento general de la aplicación y la experiencia del usuario.
- **Pruebas de Compatibilidad y Gestión de Liberaciones Segura:** Es obligatorio realizar pruebas exhaustivas en distintos navegadores y dispositivos para garantizar la compatibilidad. Además, el proceso de liberación debe incluir controles que permitan despliegues seguros y efectivos, con la capacidad de revertir cambios si es necesario.
- **Operaciones de Healthcheck:** Deben implementarse procedimientos para monitorear la salud de la interfaz web, asegurando la alta disponibilidad y el correcto funcionamiento del sistema.

5. Desarrollo del Backend y Servicios

Los servicios de backend son fundamentales para procesar, gestionar y almacenar datos de manera eficiente, proporcionando así una base sólida para todas las operaciones de la aplicación. A continuación, se detallan los requerimientos técnicos específicos para el desarrollo de estos servicios:

Lenguajes de Programación Estándar:

Se debe optar por lenguajes de programación establecidos y ampliamente utilizados como Java, JavaScript (específicamente Node.js para operaciones de backend) y Python. Estos lenguajes son seleccionados por su robustez, extensa comunidad de soporte y la disponibilidad de numerosas bibliotecas y frameworks que facilitan el desarrollo eficiente.

Prácticas de Desarrollo y Mantenimiento:

- **Control de Versión:** Implementar control de versiones a través de herramientas como Git para manejar eficientemente el desarrollo colaborativo y mantener un historial detallado de cambios.
- **Pruebas Automatizadas:** Establecer un régimen riguroso de pruebas automatizadas para asegurar la calidad y funcionamiento del software antes de su despliegue.
- **Integración y Entrega Continuas (CI/CD):** Adoptar prácticas de CI/CD para automatizar las pruebas y el despliegue de actualizaciones, reduciendo errores y mejorando la eficiencia operativa.

6. Requerimientos de Base de Datos y Almacenamiento

El almacenamiento efectivo y seguro de datos es crucial para el funcionamiento del nuevo sistema, que maneja información sensible y documentos asociados a las solicitudes de seguridad social. Este apartado del pliego de requerimientos define las especificaciones para los sistemas de almacenamiento de datos estructurados y documentos.

Requerimientos para la Base de Datos de Datos Estructurados:

- **Tipo de Base de Datos:** La solución debe incluir una base de datos SQL, reconocida por su estabilidad, confiabilidad y robustez en la gestión de grandes volúmenes de datos. Las opciones recomendadas incluyen MySQL, PostgreSQL o sistemas equivalentes.
- **Seguridad de la Base de Datos:** Es imperativo que la base de datos implemente funcionalidades de seguridad avanzadas, incluyendo:
  - Cifrado de datos en reposo para proteger la información almacenada.
  - Controles de acceso basados en roles para gestionar quién puede ver o modificar los datos.

- Auditorías completas de acceso para rastrear y registrar todas las interacciones con los datos.

Requerimientos para el Almacenamiento de Documentos y Archivos:

- **Sistema de Gestión de Archivos:** Se requiere un sistema para el almacenamiento, indexación y recuperación eficiente de documentos, tales como imágenes y PDFs. Este sistema debe:
  - Permitir el cifrado de los documentos almacenados para garantizar su seguridad.
  - Asegurar que sólo los usuarios autorizados tengan acceso a los archivos mediante controles de acceso robustos.
  - Integrarse de manera fluida con la arquitectura general de la aplicación, apoyando operaciones básicas de gestión documental sin requerir las funcionalidades de un sistema de gestión documental completo.

Provisión y Gestión a través del Proveedor Cloud:

- **Administración por el Proveedor Cloud:** Tanto la base de datos como el sistema de gestión de archivos deben ser alojados y administrados por el proveedor de servicios en la nube, para aprovechar la escalabilidad, alta disponibilidad y las capacidades de recuperación ante desastres que ofrece la tecnología en la nube.

7. Requerimientos de Acceso e Identificación de Usuarios y Aplicaciones

La integridad del acceso y la autenticación son fundamentales para la seguridad del nuevo sistema. Los requerimientos especificados a continuación detallan los sistemas necesarios para gestionar la identidad y el acceso de los usuarios finales y las aplicaciones de los países miembros.

Sistema de Gestión de Identidades:

- **Validación de Identidad:** El sistema debe ser capaz de validar las credenciales de usuarios y aplicaciones, asegurando que solo las entidades autorizadas puedan acceder al sistema. Este proceso incluirá la verificación de la autenticidad de las credenciales presentadas en el punto de acceso.
- **Unificación del Acceso:** Debe proporcionarse un método coherente y seguro para acceder al sistema, ya sea mediante una interfaz web para

usuarios finales o a través de APIs para aplicaciones internas, manteniendo un control centralizado y robusto sobre los accesos al sistema.

Autenticación y Autorización:

- **Centralización de la Autenticación:** El sistema de gestión de identidades debe centralizar la autenticación, proporcionando un único punto de verdad para verificar usuarios y aplicaciones.
- **Asignación de Roles y Permisos:** Se debe implementar un sistema de control de acceso basado en roles, que defina el nivel de acceso y las operaciones permitidas para cada usuario o aplicación, aplicando el principio de mínimo acceso y segregación de funciones.

Gestión de Tokens de Acceso:

- **Emisión y Gestión de Tokens:** El sistema debe generar y distribuir tokens de acceso seguros tras una autenticación exitosa. Estos tokens servirán como credenciales temporales para operar dentro del sistema.
- **Revocación y Validación de Tokens:** Debe existir un mecanismo para la rápida revocación y validación de tokens, asegurando que los accesos no autorizados sean eficazmente neutralizados.

Autenticación Multifactor (MFA):

- **Implementación de MFA:** Se debe implementar la autenticación multifactor como un requisito estándar para todos los usuarios, especialmente aquellos con acceso a datos sensibles. La MFA añadirá una capa adicional de seguridad al proceso de autenticación.
- **Flexibilidad y Configuración:** El sistema MFA debe ser configurable para adaptarse a diversas necesidades de seguridad y cumplir con las regulaciones específicas aplicables.

Registro y Monitoreo de Actividades:

- **Auditoría de Seguridad:** El sistema debe registrar todas las acciones realizadas por los usuarios y aplicaciones, incluyendo detalles de acceso y transacciones. Esto es crucial para la auditoría de seguridad, el cumplimiento normativo y la detección de actividades sospechosas o anomalías.

8. Requerimientos de Seguridad y Cifrado

La seguridad y el cifrado de la información son aspectos críticos para el nuevo sistema, dada la naturaleza sensible de los datos manejados, que incluyen información personal y detalles críticos de ciudadanos de múltiples países. Los siguientes requisitos deben cumplirse para asegurar la integridad y la confianza en el sistema de intercambio de información:

Cifrado de Datos en Tránsito:

- **Implementación de TLS (Transport Layer Security):** Todos los datos transmitidos entre la aplicación y los usuarios o entre sistemas internos deben estar protegidos mediante TLS para prevenir la interceptación y el acceso no autorizado. Esto es crucial para la información que circula a través de redes potencialmente inseguras.

Cifrado de Datos en Reposo:

- **Uso de Algoritmos de Cifrado Robustos:** Los datos almacenados en bases de datos, sistemas de archivos o cualquier otro medio deben estar cifrados utilizando algoritmos de cifrado reconocidos por la industria para garantizar que, incluso en caso de acceso físico no autorizado, la información se mantenga segura e inaccesible.

Gestión Segura de Claves de Cifrado:

- **Servicio de Gestión de Claves:** Debe implementarse un servicio de gestión de claves para la generación, almacenamiento, rotación y revocación de claves de forma segura y controlada, asegurando la efectividad del cifrado a lo largo del tiempo.

Seguridad en la Interfaz Web y APIs:

- **HTTPS/TLS para la Interfaz Web y APIs:** Todas las comunicaciones a través de la interfaz web y las APIs deben emplear HTTPS/TLS, garantizando que los datos transmitidos estén cifrados y protegiendo la privacidad e integridad de la información.
- **Firewall de Aplicaciones Web (WAF):** Se debe incorporar un WAF para filtrar y bloquear amenazas dirigidas específicamente a la interfaz web, reforzando la defensa contra vulnerabilidades comunes.
- **Manejo Seguro de Sesiones y Cookies:** Implementar prácticas seguras en la gestión de sesiones y cookies, incluyendo timeouts de sesión adecuados y almacenamiento protegido de tokens.

Seguridad Operativa y Auditorías:

- **Auditoría y Control de Acceso:** Implementar mecanismos de auditoría para monitorear el uso de las claves de cifrado y controlar el acceso a estas.
- **Pruebas de Penetración y Análisis de Vulnerabilidades:** Realizar análisis de vulnerabilidades y pruebas de penetración regularmente para identificar y mitigar riesgos potenciales antes de la puesta en producción.

Cumplimiento Normativo y Certificaciones:

- **Adherencia a Estándares Internacionales:** El sistema debe cumplir con normativas internacionales de protección de datos como GDPR, HIPAA u otras aplicables, utilizando tecnologías y procedimientos que estén en conformidad con estos estándares.

3.3 Requerimientos de Confidencialidad, Protección de Datos y Legalidad en Materia de Alojamiento Cloud

En el desarrollo de la nueva aplicación, es crucial abordar adecuadamente la confidencialidad y la protección de datos personales, especialmente debido a la diversidad de marcos regulatorios en los países involucrados. La aplicación será utilizada por países de América Latina, que pueden tener variados grados de regulación en materia de protección de datos, y por países de la Unión Europea, como España y Portugal, que siguen el Reglamento General de Protección de Datos (RGPD) de la UE. Por tanto, se requiere un enfoque que no solo cumpla con la legislación local, sino que también respete los estándares más estrictos establecidos por la UE.

Requerimientos Específicos:

- **Cumplimiento Normativo Mínimo de la UE:** Dado que el RGPD establece uno de los marcos de protección de datos más rigurosos del mundo, todos los aspectos del sistema, incluido el alojamiento cloud, deben cumplir al menos con estos estándares como límite mínimo de garantía de protección de datos. Esto garantizará que la aplicación sea adecuada para el uso en todos los países involucrados, independientemente de las diferencias locales en la legislación de protección de datos.
- **Selección de Proveedor Cloud y Localización de Datos:**
  - **Proveedor Cloud Conforme con RGPD:** El proveedor de servicios cloud seleccionado debe demostrar cumplimiento con el RGPD y

preferiblemente tener certificaciones que validen su capacidad para manejar datos de manera segura y conforme a las regulaciones.
    - **Localización de los Datos:** Los datos deben almacenarse preferentemente en jurisdicciones que cumplen con el RGPD o que han sido reconocidas por la Unión Europea como poseedoras de un nivel adecuado de protección de datos. Esto asegura que los datos no solo se almacenan legalmente, sino que también están protegidos contra accesos no autorizados o transferencias ilegales.
- **Acuerdos de Nivel de Servicio (SLAs):**
    - Los SLAs con el proveedor cloud deben especificar claramente las responsabilidades en términos de protección de datos, incluyendo medidas de seguridad, gestión de brechas de datos y derechos de auditoría por parte de la OISS o las autoridades reguladoras pertinentes.
    - Debe establecerse un mecanismo de respuesta rápida para cualquier incidente de seguridad que pueda afectar la integridad o la confidencialidad de los datos personales.

4. Metodología de trabajo

El éxito en el desarrollo de la nueva aplicación depende crucialmente de la adopción de una metodología de trabajo estructurada y efectiva que garantice la calidad, la eficiencia y la colaboración efectiva entre todos los equipos involucrados. A continuación, se especifican los requerimientos para las metodologías de desarrollo, pruebas y gestión de proyectos que deberán seguirse en el proceso de creación de la aplicación.

Metodología de Desarrollo:

- **Enfoque Ágil:** El desarrollo del proyecto deberá seguir una metodología ágil que permita la flexibilidad en la planificación, el desarrollo iterativo y evolutivo, y una comunicación constante con los stakeholders. Métodos como Scrum o Kanban serán preferidos para facilitar estos procesos.
- **Revisión Continua y Adaptación:** Los ciclos de desarrollo cortos y las reuniones regulares de revisión del progreso (Sprints) permitirán ajustes rápidos a los requerimientos y soluciones basadas en el feedback continuo de los usuarios y los miembros del equipo.
- **Colaboración y Comunicación:** Deberá fomentarse una colaboración estrecha entre desarrolladores, diseñadores, administradores de sistemas y usuarios finales para asegurar que todos los aspectos del sistema sean considerados y que el producto final cumpla con las necesidades de todos los usuarios.

Gestión de Pruebas:

- **Pruebas Automatizadas:** Implementar un amplio conjunto de pruebas automatizadas, incluyendo pruebas unitarias, pruebas de integración y pruebas de aceptación de usuario, para asegurar la calidad y el funcionamiento del software en todas las etapas del desarrollo.
- **Involucración del Usuario:** Realizar pruebas de aceptación con usuarios reales para asegurarse de que el sistema cumple con sus expectativas y es capaz de realizar las tareas requeridas de manera efectiva.

Control de Versiones y Documentación:

- **Control de Versiones:** Utilizar sistemas de control de versiones como Git para manejar y documentar todos los cambios en el código fuente. Esto facilitará la colaboración entre equipos, el seguimiento de cambios y la restauración de versiones anteriores si es necesario.
- **Documentación Exhaustiva:** Mantener una documentación detallada y actualizada de todo el código, las configuraciones y las arquitecturas utilizadas.

Gestión de Proyectos:

- **Herramientas de Gestión de Proyectos:** Emplear herramientas de gestión de proyectos como Jira, Trello o Asana para planificar, supervisar y reportar sobre el progreso del proyecto. Estas herramientas ayudarán a mantener a todos los miembros del equipo alineados y centrados en los objetivos del proyecto.
- **Entregables y Hitos:** Definir claramente los entregables y los hitos del proyecto, estableciendo expectativas claras para cada fase del desarrollo. Los hitos deben ser medibles y alcanzables, y cada entrega debe ser evaluada meticulosamente antes de ser considerada completa. La Comisión Informática del Comité Técnico Administrativo del CMISS acompañará este proceso.

5. Alcance funcional de la aplicación

La nueva aplicación se centrará en el desarrollo de formularios de envío y respuesta que faciliten un intercambio eficaz y seguro de información entre los países miembros, siguiendo los formularios ya aprobados por el Comité Técnico Administrativo del CMISS (en la actualidad son 10 y en el futuro podrían acordarse más). La nueva aplicación se desarrollará siempre dentro del marco descrito en el documento acordado por el Comité Técnico Administrativo, que se incluye como Anexo I. Los formularios son aprobados por el Comité Técnico Administrativo del CMISS y la información requerida en los mismos solo puede ser modificada por el propio comité.

A continuación, se detalla el contenido funcional y la estructura que deben tener estos formularios (ver formularios en https://oiss.org/convenio-multilateral/formularios/):

Formulario de Envío:

- **Información sobre la solicitud de prestaciones:** Debe permitir seleccionar el tipo de prestación solicitada con opciones predefinidas (jubilación por edad, invalidez, pensión por muerte, etc.) según cada uno de los formularios acordados, incluir la fecha de la solicitud y un número de expediente para seguimiento.
- **Datos del trabajador asegurado:** Sección para ingresar datos completos del trabajador, incluyendo campos obligatorios y específicos según la entidad receptora, según los formularios acordados.
- **Otros documentos del trabajador asegurado:** Capacidad para adjuntar documentos adicionales relacionados con el trabajador, según los formularios acordados.
- **Datos del solicitante (para pensiones de supervivencia):** Información detallada del solicitante en caso de pensiones de supervivencia, según los formularios acordados.
- **Períodos de seguro, cotización o empleo:** Detalles sobre el historial laboral del solicitante, necesario para la evaluación de la solicitud, según los formularios acordados.

Formulario de Respuesta:

- **Organismo de enlace o institución competente que tramita el procedimiento:** Incluirá información precargada del formulario enviado, con campos bloqueados para evitar modificaciones.
- **Información sobre la solicitud de prestaciones:** Mostrará datos de la solicitud con campos bloqueados, proporcionando un contexto claro sobre la solicitud original.
- **Datos del asegurado:** Incluirá información del asegurado con la mayoría de los campos bloqueados pero permitirá añadir detalles en "Otras informaciones".
- **Información exclusiva para solicitud de pensión por incapacidad y pensiones de supervivencia:** Secciones específicas que contienen datos pertinentes a cada tipo de solicitud, con campos precargados y limitados para edición.
- **Certificación de períodos de seguro, cotización o empleo:** Permite la adición de nuevos períodos o la certificación de los existentes, esencial para validar la solicitud.
- **Totales cotizados:** Sección para calcular el total de períodos cotizados una vez que se hayan ingresado todos los datos relevantes.

- **Prestaciones a cargo de la institución que tramita el procedimiento:** Sección para detallar las prestaciones responsabilidad de la institución, incluyendo si son por totalización.

Detalle de las Informaciones a Intercambiar:

- **Tipos de prestaciones solicitadas:** Detallar claramente las diferentes opciones de prestaciones para que los usuarios puedan seleccionar adecuadamente.
- **Datos históricos laborales y personales del asegurado y del solicitante:** Es fundamental para la evaluación de las solicitudes.
- **Documentación adicional requerida:** Debe soportar la carga de documentos necesarios para cada tipo de solicitud.
- **Información bloqueada y editable en formularios de respuesta:** Claridad sobre qué información viene precargada y qué puede ser añadida o certificada, para mantener la integridad de la información intercambiada.

6. Requerimientos de proveedor y personal

6.1 Perfil del Proveedor

- **Experiencia y capacidades requeridas:**
  - **Experiencia demostrable en desarrollo de sistemas complejos:** El proveedor debe haber completado con éxito proyectos de desarrollo de sistemas similares en tamaño y complejidad, preferiblemente en el sector público o en entornos multilaterales que involucren múltiples países o jurisdicciones.
  - **Capacidad técnica en arquitecturas modernas:** Profunda experiencia en la implementación de soluciones basadas en microservicios o arquitecturas monolíticas optimizadas, con un fuerte enfoque en la escalabilidad, seguridad y rendimiento.
  - **Experiencia en entornos cloud y con proveedores de servicios cloud principales (Amazon AWS, Google Cloud Platform, Microsoft Azure):** Competencia comprobada en la configuración y gestión de infraestructuras cloud, preferentemente con certificaciones oficiales de dichos proveedores.
  - **Cumplimiento de estándares de seguridad y protección de datos:** Experiencia demostrada en la implementación de soluciones que cumplen con altos estándares de seguridad, incluyendo encriptación de datos, autenticación robusta, y cumplimiento de normativas internacionales de protección de datos.

6.2 Perfil del Personal

- **Descripción de los perfiles profesionales necesarios:**
  - **Arquitecto de Soluciones:** Encargado de diseñar la arquitectura general del sistema, asegurando que todas las componentes funcionen de manera coherente y eficiente. Debe tener experiencia en diseño de arquitecturas tanto de microservicios como monolíticas y estar familiarizado con las prácticas de desarrollo y despliegue en la nube.
  - **Desarrolladores de Software:** Profesionales con experiencia en los lenguajes de programación especificados (Java, JavaScript, Python) y con habilidades en frameworks modernos de desarrollo frontend y backend como React, Angular, Spring Boot, entre otros.
  - **Ingenieros de Seguridad en TI:** Especialistas en la implementación de medidas de seguridad a nivel de aplicación y de datos, con experiencia en técnicas de cifrado, autenticación y cumplimiento de estándares de seguridad internacionales.
  - **Analista de Datos:** Responsable de manejar la integración, procesamiento y seguridad de los datos intercambiados a través de la aplicación, con conocimientos en bases de datos y almacenamiento en la nube.
  - **Gestor de Proyecto:** Con experiencia en gestión de proyectos de TI de gran escala, preferiblemente con certificaciones como PMP o equivalentes. Debe tener habilidades probadas en la coordinación de equipos multidisciplinarios y multiculturales.
- **Cualificaciones y experiencia esperada:**
  - **Certificaciones relevantes:** Se espera que el personal tenga certificaciones pertinentes en sus áreas de especialización, como certificaciones de desarrollador/ arquitecto de los principales proveedores de servicios cloud, certificaciones de seguridad (CISSP, CISM) o certificaciones de gestión de proyectos (PMP, Agile, etc.).
  - **Experiencia en proyectos similares:** Es crucial que el personal tenga experiencia previa trabajando en proyectos de desarrollo con un enfoque particular en aplicaciones que manejan información sensible y requieren altos estándares de confiabilidad y seguridad.
  - **Habilidades de comunicación y trabajo en equipo:** Dada la naturaleza del proyecto y su alcance multilateral, se valoran altamente las habilidades de comunicación efectiva y la capacidad de trabajar en equipos distribuidos geográficamente.

7. Criterios de adjudicación

Para la adjudicación del contrato para el desarrollo de la nueva aplicación, los criterios de valoración se dividirán en criterios cuantificables mediante fórmulas y criterios sometidos a juicio de valor, asignando un total de 100 puntos distribuidos en una proporción de 60/40.

1. **Criterios Cuantificables mediante Fórmulas (60 puntos en total)**
    - **Precio (40 puntos):** La oferta económica más baja recibirá la puntuación completa, y las otras ofertas recibirán puntos de manera proporcional según su cercanía al precio más bajo.
    - **Certificaciones o Acreditaciones Profesionales (5 puntos):** Se valorarán certificaciones relevantes del personal del licitador en áreas como programación segura, gestión de la seguridad de la información y tecnologías de desarrollo cloud.
    - **Experiencia en Proyectos con Cifrado o Seguridad de Datos y en Desarrollo Cloud (10 puntos):** Se valorará la experiencia previa del licitador en la implementación de proyectos que requieran extenso uso de cifrado y medidas de seguridad de datos avanzadas, así como su competencia en el desarrollo de soluciones basadas en la nube.
    - **Ampliación de Garantía (5 puntos):** Se valorará positivamente la extensión de la garantía ofrecida por encima de los seis meses requeridos, asignando un punto adicional por cada mes de garantía hasta un máximo de cinco puntos.
2. **Criterios Sometidos a Juicio de Valor (40 puntos en total)**
    - **Planteamiento del Proyecto y Calendario de Tareas (10 puntos):** Evaluación de la propuesta de gestión del proyecto del licitador, incluyendo la planificación de tareas, la metodología de implementación y la capacidad para cumplir con los plazos establecidos.
    - **Propuesta de Proveedor Cloud y Especificaciones de la Arquitectura (30 puntos):** Valoración de la propuesta del licitador para la selección del proveedor cloud, incluyendo una descripción detallada de la arquitectura propuesta, los productos de cloud a utilizar, el coste total estimado y los SLAs propuestos. Esta evaluación considerará cómo estas elecciones cumplen con las especificaciones técnicas y de seguridad definidas en el pliego.

Metodología de Valoración

- **Puntuación Proporcional para el Precio:** Se aplicará la fórmula *Vof*=40×(Precio de la OfertaPrecio Ma´s Bajo Ofertado) para asignar puntos a las ofertas económicas.

Vof=40×(Precio Ma´s Bajo OfertadoPrecio de la Oferta)

- **Evaluación de Propuestas Técnicas:** Los criterios de juicio de valor serán evaluados por un comité de expertos que revisará y puntuará las propuestas en función de su calidad técnica, el cumplimiento de los requisitos y la innovación mostrada en la solución propuesta.

Implementación de la Valoración

- Los licitadores deberán presentar toda la documentación necesaria que justifique su puntuación en los criterios cuantificables, incluyendo detalles y certificados de las certificaciones profesionales y descripciones de proyectos anteriores relevantes.
- Para los criterios de juicio de valor, se requerirá que los licitadores presenten una propuesta detallada que incluya planes técnicos, cronogramas, especificaciones del proveedor cloud elegido, y un desglose del coste y SLAs.

8. Duración y garantía del contrato

El contrato para el desarrollo de la nueva aplicación tendrá una duración total de 18 meses, contados a partir de la fecha especificada en el documento contractual o desde el acto de inicio del proyecto (kick off). Este período se estructura de la siguiente manera:

- **Periodo de Desarrollo:** 12 meses desde la fecha de inicio, durante los cuales se llevarán a cabo todas las fases de desarrollo del sistema, incluyendo la planificación, ejecución, pruebas y finalización de los desarrollos necesarios.
- **Periodo de Garantía:** Un mínimo de 6 meses de garantía post-desarrollo, comenzando inmediatamente después de la finalización del periodo de desarrollo.

Inicio de las Tareas: La fecha de inicio de las tareas del proyecto se acordará entre ambas partes y no será posterior a los quince días naturales desde la fecha de formalización del contrato, a menos que el retraso sea imputable al adjudicatario.

Garantía de la Solución:

- La empresa adjudicataria deberá proporcionar un periodo de garantía de seis meses a partir de la conclusión del periodo de desarrollo de 12 meses.
- Durante la garantía, el proveedor se comprometerá a realizar el soporte necesario para solventar cualquier deficiencia detectada que sea imputable a su gestión o errores en el desarrollo.

- La garantía incluirá la corrección de errores y fallos manifiestos en el funcionamiento del sistema, así como la conclusión y corrección de la documentación que sea incompleta o presente deficiencias.

Servicio y Soporte Durante la Garantía:

- El proveedor deberá comprometerse a ofrecer un servicio de atención tipo 8x5, cubriendo la resolución de incidencias durante el horario laboral de lunes a viernes, excepto festivos, con un tiempo de respuesta máximo de 2 horas desde la notificación de la incidencia.

Documentación de los Trabajos:

- El adjudicatario se compromete a generar toda la documentación necesaria según la metodología establecida por la OISS, la cual quedará en propiedad exclusiva de la OISS, al igual que la propiedad intelectual y los derechos de cualquier tipo de uso del producto desarrollado. El proveedor no podrá conservar, copiar ni distribuir dicha documentación sin autorización expresa de la OISS.

Gestión del Proyecto:

- La OISS designará un Jefe de Proyecto responsable del control y supervisión del cumplimiento de los programas y objetivos establecidos para el proyecto.
- El Jefe de Proyecto también será responsable de la comunicación efectiva con los usuarios finales y de supervisar la calidad de los productos entregados.
- Será función del Jefe de Proyecto identificar problemas, proponer la participación de expertos funcionales y organizar la formación de usuarios según sea necesario.
- El adjudicatario mantendrá una comunicación fluida con el Jefe de Proyecto durante todas las etapas del mismo.
- Dado que el Comité Técnico Administrativo del CMISS deberá aprobar el uso definitivo de este sistema, se realizarán presentaciones periódicas de los avances al mismo y se incluirán los cambios solicitados por aquel.

9. Términos y condiciones generales

Confidencialidad:

- El proveedor se compromete a mantener la confidencialidad de toda información clasificada como confidencial que se le proporcione durante la ejecución del contrato. Esto incluye, sin limitación, información técnica, operativa, comercial, financiera y personal.

- Esta obligación de confidencialidad persistirá incluso después de la finalización o rescisión del contrato.

Propiedad Intelectual:

- Todos los derechos de propiedad intelectual generados como resultado del desarrollo de la nueva aplicación serán propiedad exclusiva de la OISS.
- El proveedor garantiza que los materiales y tecnologías utilizados en el desarrollo de la aplicación son originales, no infringen derechos de terceros y tiene pleno derecho para utilizarlos en el marco del proyecto.
- Se requerirá que el proveedor otorgue a la OISS una licencia ilimitada para usar, modificar, y distribuir cualquier software, documentación y demás materiales desarrollados durante el proyecto.

Modificación y terminación del Contrato:

- Cualquier modificación al contrato debe ser realizada por escrito y firmada por ambas partes.
- El contrato podrá ser rescindido por la OISS unilateralmente y sin derecho a indemnización si el proveedor incumple con cualquiera de los términos y condiciones establecidos, incluyendo, pero no limitándose a, fallas en cumplir con los cronogramas de entrega o los estándares de calidad requeridos.
- La rescisión puede ser efectuada sin perjuicio de cualquier otro derecho o recurso que la OISS pueda tener bajo las leyes aplicables o bajo otras cláusulas del contrato.

10. Presupuesto

La cuantía máxima que podrá presupuestarse para la realización completa de este proyecto será de **150.000 € (ciento cincuenta mil euros)**, impuestos y costes de transferencias incluidos. El abono de esta cuantía se realizará según se completen los hitos del proyecto que se acuerden al inicio del mismo.

11. Presentación de propuestas

Las propuestas deberán incluir toda la documentación necesaria que justifique su puntuación en los criterios cuantificables, incluyendo detalles y certificados de las certificaciones profesionales y descripciones de proyectos anteriores relevantes.

Para los criterios de juicio de valor, se requerirá que los licitadores presenten una propuesta detallada que incluya planes técnicos, cronogramas, especificaciones del proveedor cloud elegido, y un desglose del coste y SLAs.

Las propuestas deberán remitirse por correo electrónico a sec.general@oiss.org **antes del 30 de junio de 2024.**