PROPUESTA DE ARQUITECTURA PARA DESARROLLO DE NUEVO SISTEMA DE TRANSFERENCIA DIGITAL DE INFORMACIÓN DE PRESTACIONES AL AMPARO DEL CMISS

Versión 1.0 12/01/2024

INDICE DE CONTENIDO

Con el apoyo:

INTRODUCCIÓN

El presente informe tiene como finalidad principal exponer de manera exhaustiva los requerimientos tecnológicos, así como la arquitectura técnica y funcional, necesarios para el diseño y desarrollo de un sistema avanzado de transferencia electrónica internacional de información (en adelante, el "nuevo sistema") para la tramitación de prestaciones en el ámbito del Convenio Multilateral Iberoamericano de Seguridad Social (en adelante, el "Convenio"). En el marco de este Convenio, se busca facilitar y agilizar el proceso de gestión, reconocimiento y abono de prestaciones relacionadas con invalidez, vejez, supervivencia, accidentes de trabajo y enfermedad profesional a través del intercambio eficiente de formularios y documentación justificativa entre las instituciones de los Estados Parte.

El sistema propuesto aspira a suceder y superar a la aplicación previa, conocida como SIBERO, incorporando mejoras significativas basadas en las deficiencias detectadas y sugerencias de optimización planteadas durante la reunión de la Comisión Informática del Convenio, celebrada en Montevideo el 30 de octubre de 2023. Las recomendaciones y la estructura propuesta para la nueva arquitectura de la aplicación fueron presentadas y preliminarmente aprobadas en las sesiones de videoconferencia con los países miembros del Convenio realizadas los días 15 y 21 de diciembre de 2023.

Este documento detalla dicha arquitectura y recopila consideraciones clave aportadas en dichas reuniones, con el objetivo de brindar una visión integral y detallada que sirva de base para la valoración técnica por parte de los países involucrados. La meta es, tras un proceso de evaluación y ajustes conjuntos, convertir esta documentación en un pliego de requerimientos riguroso que facilite la posterior convocatoria y adjudicación de un concurso público destinado a la contratación del desarrollo e implementación de esta solución tecnológica.

CRITERIOS PREVIOS

Esta sección establece los criterios que han sido fundamentales en la definición de la arquitectura y las soluciones tecnológicas y funcionales detalladas en este informe. Estos criterios han servido como directrices durante el proceso de diseño, asegurando que cada aspecto de la solución propuesta esté alineado con las necesidades específicas, objetivos y contexto operativo del sistema de transferencia electrónica internacional de información. Han influido en la selección de tecnologías, en la configuración de la infraestructura y en la determinación de los protocolos de seguridad y operatividad, conformando así una base cohesiva para las decisiones técnicas y funcionales que se describen en las siguientes secciones del documento. La comprensión de estos criterios es esencial para apreciar la lógica detrás de la arquitectura propuesta y las recomendaciones tecnológicas incluidas en este informe.

Implementación Cloud en PaaS

La Organización Iberoamericana de la Seguridad Social (OISS), en tanto que secretaría del Comité Técnico Administrativo del Convenio Multilateral Iberoamericano de Seguridad Social y como mandatada por este Comité para el desarrollo del sistema de transferencia digital de información, enfrenta limitaciones en términos de infraestructura tecnológica y recursos humanos especializados para la gestión y operación de sistemas informáticos complejos. Esta realidad impone la necesidad de una solución que minimice la carga operativa y técnica sobre la organización mientras proporciona una plataforma robusta y flexible para la tramitación de prestaciones. En este sentido, se ha optado por una solución basada en Plataforma como Servicio (PaaS), la cual elimina la necesidad de gestionar y mantener la infraestructura subyacente, centrando los esfuerzos en el desarrollo y mejora continua de la aplicación. Esta aproximación asegura que la OISS pueda proveer servicios eficientes y seguros sin incurrir en las complejidades asociadas con la gestión directa de los recursos de TI. Dado el enfoque en una implementación de PaaS, se requiere la selección cuidadosa de un proveedor que no solo ofrezca un alto grado de disponibilidad y escalabilidad automática sino también una suite integral de herramientas de desarrollo y gestión que permitan acelerar el ciclo de vida del software.

Interfaz de Usuario y Acceso API

Conforme a los acuerdos de la Comisión Informática del 30 de octubre de 2023, la aplicación deberá implementar un modelo mixto que soporte tanto la integración B2B (Business to Business), permitiendo la interconexión y operación automática entre sistemas de diferentes instituciones, como el acceso directo B2C (Business to Consumer), para los usuarios finales que gestionan o consultan prestaciones. Para asegurar una amplia adopción y eficiencia en la tramitación de prestaciones, la aplicación, por lo tanto, debe ser altamente accesible y operativa tanto para usuarios finales a través de una interfaz web como para sistemas automatizados mediante APIs (Application Programming Interfaces). La interfaz de usuario debe ser intuitiva y fácil de usar para permitir a los usuarios de los distintos países interactuar eficientemente con el sistema. Paralelamente a la interfaz web, la aplicación debe ofrecer un conjunto de APIs bien documentadas y seguras que permitan la integración con sistemas externos. Estas APIs deben seguir principios de diseño RESTful (Representational State Transfer), ofreciendo una interfaz coherente, eficiente y fácil de usar para la automatización de procesos y la integración con otras plataformas y servicios. Esto implica un enfoque flexible y modular en el diseño de la aplicación, asegurando que ambos modos de operación se implementen de manera efectiva y coherente.

Expertise y Competitividad: Criterios de Selección Tecnológica

En un contexto de desarrollo de aplicaciones complejas y de gran alcance como lo es un sistema internacional de transferencia de información, la selección de tecnologías juega un papel crucial. Se busca priorizar la adopción de tecnologías maduras y ampliamente soportadas que aseguren la agilidad y estabilidad de la aplicación. La elección consciente de estas tecnologías permite no solo una implementación más rápida y segura sino también un mantenimiento más eficiente y una mayor facilidad en la futura escalabilidad de la solución. Asimismo, la preferencia por tecnologías con un amplio reconocimiento y base de usuarios facilita la contratación de personal con el “expertise” necesario y la selección de empresas con experiencia probada en su implementación. Preferir tecnologías que, por su madurez y popularidad, cuenten con una amplia oferta de proveedores y empresas de desarrollo no solo aumenta las opciones disponibles al momento de realizar licitaciones y contrataciones, sino

que también promueve condiciones más competitivas en términos de costos y calidad del servicio.

Uso de Servicios Gestionados y Soporte del Proveedor Cloud

En el contexto de una implementación en la nube, el uso de servicios gestionados emerge como una estrategia fundamental para maximizar la eficiencia operativa y reducir la complejidad técnica. La utilización de estos servicios permite a la OISS concentrarse en las funcionalidades y objetivos de la aplicación, dejando en manos del proveedor cloud la gestión, mantenimiento y escalabilidad de los componentes tecnológicos críticos. Esta aproximación reduce significativamente la necesidad de recursos técnicos especializados para la administración de sistemas y bases de datos, la gestión de seguridad y el rendimiento de la infraestructura, lo cual es especialmente valioso dada la naturaleza intergubernamental y la distribución geográfica de la aplicación.

Optar por un proveedor cloud específico y utilizar sus productos integrados, aunque conlleve cierto grado de compromiso y dependencia, se ha decidido prioritario para garantizar tiempos ágiles de desarrollo y minimizar la complejidad en la integración y mantenimiento. La selección se basa en el entendimiento de que los beneficios inmediatos de una implementación más rápida, junto con el soporte continuo y las capacidades integradas de gestión, superan los desafíos potenciales asociados con una eventual migración a futuro, teniendo en cuenta, además, que el ecosistema de la nube está en constante evolución, con mejoras en la interoperabilidad y herramientas para facilitar la migración entre plataformas.

La preferencia por soluciones integradas y soportadas directamente por el proveedor simplifica el proceso de implementación y mantenimiento. Se seleccionarán productos y servicios que estén preconfigurados para una implementación eficiente y respaldados por un compromiso de soporte y mantenimiento, incluyendo preferentemente productos propios del proveedor o aquellos de terceros con integraciones certificadas y soporte garantizado.

Establecimiento de SLAs y Soporte de Supervisión

Asegurar una disponibilidad constante, rendimiento óptimo y un soporte técnico eficiente es crucial para el funcionamiento exitoso del sistema de intercambio de información propuesto. Los Acuerdos de Nivel de Servicio (SLAs) y un contrato claro y específico con el proveedor cloud son esenciales para establecer los estándares de servicio y las expectativas. Mientras que la contratación directa con el proveedor cloud se gestionará en un contrato separado, es fundamental que la empresa de desarrollo comprenda y esté preparada para trabajar dentro de los parámetros que estos SLAs establecerán:

- **Definición de SLAs Contractuales y Mecanismos de Supervisión:** La OISS establecerá SLAs detallados con el proveedor cloud elegido en un contrato separado. Se establecerán, además, herramientas y procedimientos para el monitoreo continuo del cumplimiento de los SLAs una vez que la aplicación esté operativa. Estos SLAs abordarán aspectos críticos como tiempo de actividad, rendimiento del sistema y tiempos de respuesta del soporte técnico, como por ejemplo:
    - Aplicación de las últimas actualizaciones de seguridad, incluyendo parches y service packs.
    - Alta disponibilidad del sistema y generación de alertas sobre incidentes de seguridad, con un registro detallado para auditorías.
    - Notificación inmediata ante incidentes que afecten a datos personales y realización de pruebas de seguridad periódicas.
    - Implementación de un plan de copias de seguridad eficiente, asegurando la rápida recuperación de datos.
    - Evaluación post-desarrollo sobre vulnerabilidades potenciales de la infraestructura seleccionada.

  La supervisión de los SLAs del proveedor cloud será responsabilidad del proveedor seleccionado durante la ejecución del proyecto y por un plazo de 6 meses tras la puesta en producción. Posteriormente, corresponderá a la OISS determinar la entidad y el método para continuar con el monitoreo y seguimiento de los SLAs de la aplicación por parte del proveedor cloud, asegurando la continuidad y eficacia del servicio.
- **Inclusión en la Propuesta de Concurso**: Aunque el contrato con el proveedor cloud será independiente, el concurso para el desarrollo de la aplicación incluirá un requisito para que las empresas ofertantes presenten una propuesta razonada del proveedor cloud y los productos específicos que pretenden utilizar para el desarrollo de la solución final.

Esta propuesta debe justificar cómo la elección del proveedor cloud y sus servicios específicos contribuirán a la eficiencia, escalabilidad, seguridad y cumplimiento de los objetivos del proyecto.

- **Evaluación Integrada para la Selección**: Las propuestas de proveedor cloud presentadas por las empresas de desarrollo se considerarán tanto en la selección del contratista para el desarrollo de la aplicación como en la elección final del proveedor cloud. Esto asegura que la solución desarrollada esté optimizada para la infraestructura cloud y que exista una alineación entre los servicios de desarrollo y cloud, facilitando una implementación fluida y eficiente.

Arquitectura basada en servicios

La implementación de una arquitectura basada en servicios desempeña un papel crucial en la modernización y eficiencia de la aplicación, al descomponer las funcionalidades en unidades más pequeñas y manejables. Esta estrategia permite una especialización funcional, donde cada servicio se centra en realizar una tarea específica o manejar un conjunto de procesos relacionados. La descomposición en servicios no solo facilita la escalabilidad y el mantenimiento, sino que también permite actualizaciones y mejoras más rápidas, contribuyendo a una respuesta ágil ante cambios o necesidades emergentes. Al diseñar los servicios para que sean consumidos tanto internamente por la interfaz web como externamente a través de APIs para acceso B2B, se maximiza la coherencia y reutilización, asegurando una arquitectura más eficiente y robusta. La reutilización de servicios no solo reduce la redundancia y el esfuerzo de desarrollo, sino que también asegura una mayor coherencia en toda la aplicación.

Continuidad de Contenido de Formularios e Información

La nueva aplicación destinada a facilitar el intercambio de información entre países miembros debe asegurar una transición fluida y sin errores del sistema existente, SIBERO, al nuevo. Es fundamental subrayar que la definición de los campos, estructuras de formularios y la naturaleza de la información a intercambiar han sido establecidos en instancias previas y, por lo tanto, no son objeto de rediscusión en el presente informe ni en el concurso de desarrollo. El objetivo es mantener la integridad y coherencia del contenido de intercambio para asegurar la continuidad operativa y la confiabilidad en los procesos de tramitación de prestaciones. Al priorizar la continuidad del contenido de intercambio, la nueva aplicación se posiciona como

una evolución natural y mejorada del sistema anterior, permitiendo a los usuarios y a las instituciones beneficiarse de una plataforma más moderna y eficiente sin tener que enfrentarse a una curva de aprendizaje pronunciada o cambios disruptivos en los procedimientos establecidos. Este enfoque asegura que la transición al nuevo sistema se realice con la mínima fricción posible, manteniendo la integridad y la confianza en los procesos de intercambio de información críticos para la tramitación de prestaciones en el marco del Convenio.

En el contexto de transición al nuevo sistema, se ha de considerar la posible migración de datos del sistema anterior. Dado el enfoque primordial del nuevo sistema en facilitar el intercambio de información sin funcionar como un repositorio de documentos, se valora que no es necesario migrar documentos o datos específicos del sistema previo, excepto la información estadística relacionada con la cantidad de intercambios históricos, para propósitos analíticos y de mejora continua.

Al concluir el desarrollo del nuevo sistema, es esencial que el proveedor adjudicatario proporcione una serie de recursos fundamentales para asegurar una transición suave y una adopción efectiva por parte de los usuarios. En este contexto, se requiere la entrega de una documentación técnica completa que detalle la arquitectura de la solución, incluyendo manuales para la instalación, configuración, y mantenimiento del sistema. Asimismo, deberán elaborarse guías de usuario final que faciliten la comprensión y el manejo cotidiano del sistema, cubriendo desde funciones básicas hasta características avanzadas. Además, el proveedor debe organizar sesiones de capacitación específicas, tanto para administradores del sistema como para usuarios finales, garantizando que todos los participantes estén plenamente preparados para operar el Nuevo Sistema de manera eficaz y segura. Estos elementos serán clave para maximizar el valor del Nuevo Sistema desde el momento de su puesta en marcha.

Seguridad y Cifrado de Información

Dada la naturaleza sensible de los datos manejados en la aplicación, que incluyen información personal y detalles críticos de ciudadanos de múltiples países, se hace imperativo garantizar la máxima confidencialidad y seguridad de estos datos en todo momento. La protección de los datos tanto en tránsito como en reposo es esencial para mantener la integridad y la confianza en el sistema de intercambio de información, evitando accesos no autorizados, filtraciones o alteraciones indebidas de la información crítica. El uso de estándares de la industria en cifrado asegura una defensa robusta frente a las amenazas y vulnerabilidades emergentes, alineándose con las mejores prácticas globales en seguridad de datos. La seguridad y el cifrado de la información no son simplemente componentes adicionales de la aplicación, sino

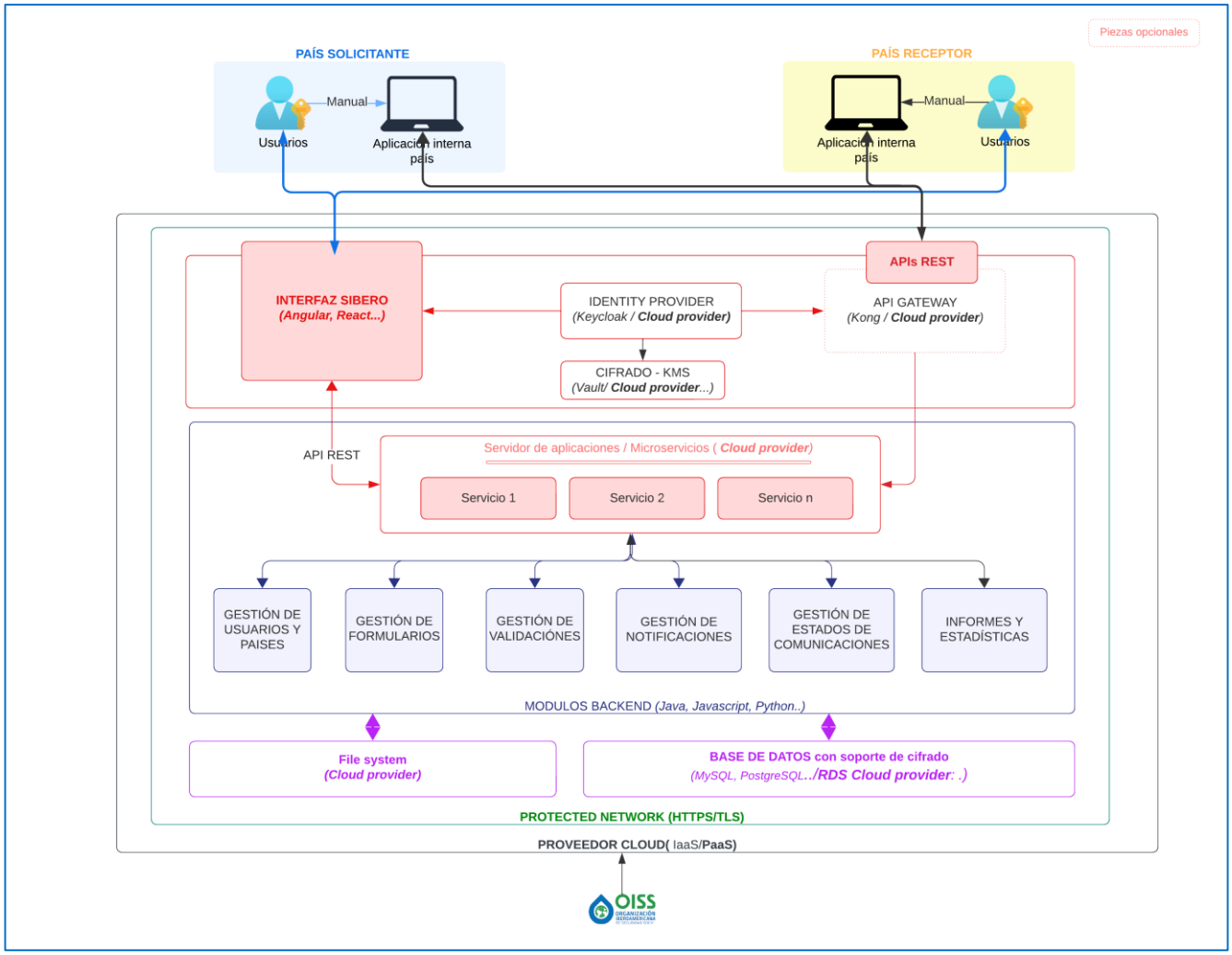
fundamentos críticos que garantizan su operatividad, confiabilidad y la confianza de los usuarios y las instituciones participantes.

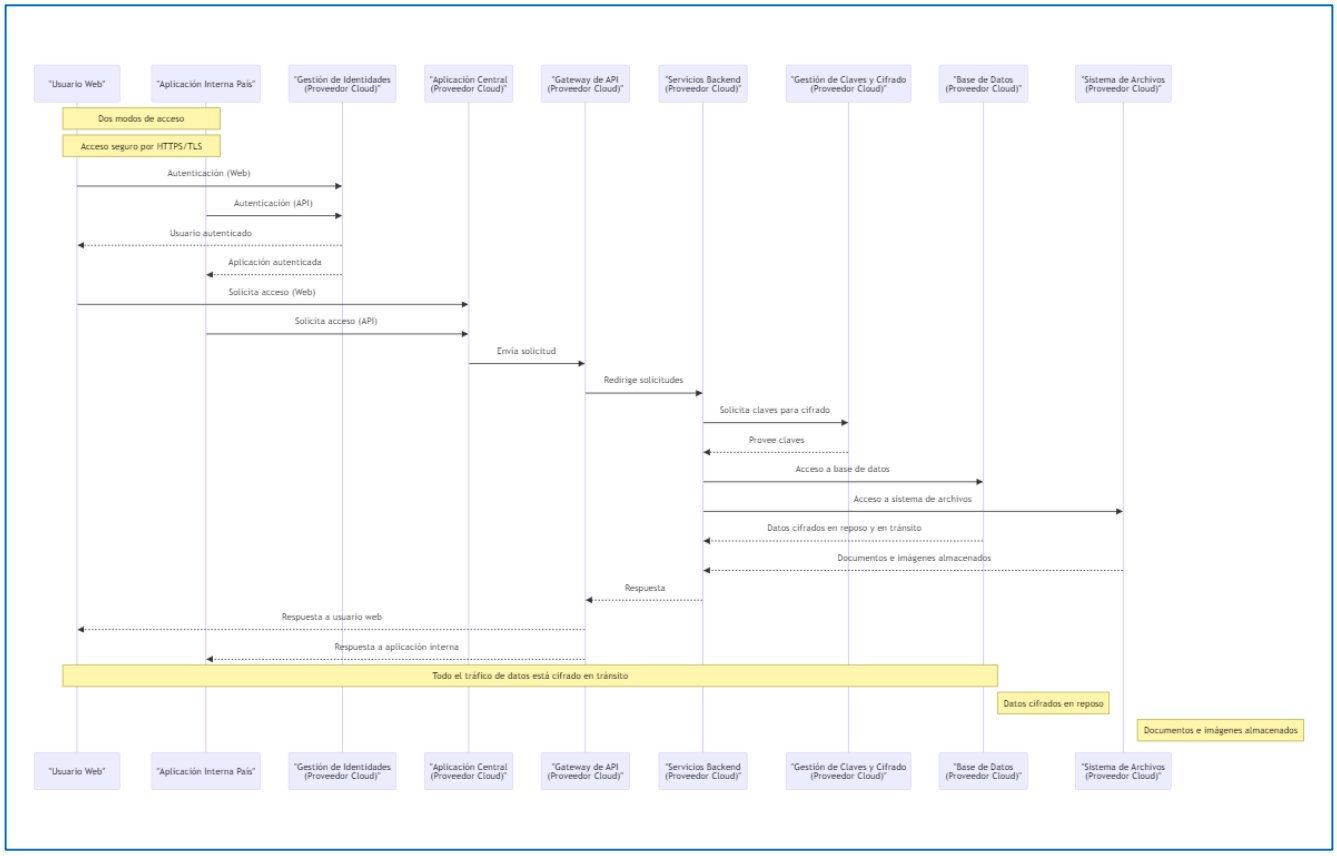
- **Cifrado de Datos en Tránsito**: Implementar protocolos de cifrado como TLS (Transport Layer Security) para asegurar que todos los datos transmitidos entre la aplicación y los usuarios o entre sistemas internos estén protegidos contra la interceptación y el acceso no autorizado. Esto es especialmente crítico para la información que se mueve a través de redes potencialmente inseguras.
- **Cifrado de Datos en Reposo**: Utilizar algoritmos de cifrado robustos para proteger los datos almacenados en bases de datos, sistemas de archivos o cualquier otro medio de almacenamiento. Este nivel de protección asegura que, incluso en caso de un acceso físico no autorizado a los datos, la información permanezca ininteligible y segura.
- **Gestión Segura de Claves de Cifrado**: Asegurar una gestión eficaz y segura de las claves de cifrado es fundamental para el cifrado efectivo. Esto debería incluir la utilización de un servicio de gestión de claves que permita la generación, almacenamiento, rotación y revocación de claves de forma segura y controlada.

Para cumplir con las expectativas de protección de datos personales, el proveedor cloud seleccionado deberá contar con certificaciones internacionalmente reconocidas como, por ejemplo, ISO 27001 para medidas técnicas de seguridad de la información, ISO 27017 para seguridad en servicios cloud,o ISO 27018 para la privacidad en el cloud, demostrando así su capacidad para gestionar de forma segura aplicaciones y servicios. Estas certificaciones son fundamentales para asegurar que la solución mantenga los más altos estándares de protección de datos

DESCRIPCIÓN DE LA ARQUITECTURA

El propósito de esta sección del informe es presentar una visión exhaustiva de la arquitectura del nuevo sistema, delineando de manera clara y precisa la función específica de cada uno de sus componentes interconectados. La exposición detallada que sigue tiene como objetivo facilitar la comprensión de cómo cada elemento contribuye al funcionamiento integral de la plataforma, destacando su rol dentro del ecosistema de la aplicación, así como su contribución a la seguridad, eficiencia y escalabilidad del sistema. Mediante el desglose de la arquitectura, buscamos ofrecer una base sólida para la apreciación técnica del diseño del sistema, así como para futuras consultas, evaluaciones y posibles desarrollos o mejoras de la plataforma.





El esqueleto del nuevo sistema se erige sobre una plataforma completamente inmersa en el paradigma de Plataforma como Servicio (PaaS), lo que significa que cada faceta del sistema, desde su concepción hasta su despliegue y mantenimiento, reside íntegramente en una infraestructura de cloud computing. Este modelo PaaS es un catalizador para la agilidad operativa y la eficiencia, proporcionando un entorno de hospedaje y desarrollo que se adapta dinámicamente a las exigencias de la aplicación y de sus usuarios. Además, posibilita una gestión simplificada de la infraestructura técnica y un escalado eficaz de recursos, acelerando así el ciclo de vida del desarrollo de software y promoviendo la innovación continua. Al avanzar hacia la selección de un proveedor de servicios en la nube para alojar el nuevo sistema, es esencial adoptar una estrategia que no solo se alinee con los objetivos técnicos y funcionales, sino que también cumpla con los criterios legales y normativos establecidos por el Convenio. Esto implica una diligencia detallada para garantizar que el proveedor de cloud seleccionado se adhiera a los requerimientos específicos relacionados con la localización de los datos, las regulaciones de protección de datos y cualquier otra obligación legal pertinente. La conformidad con dichos requisitos es un paso crítico para asegurar la validez y la legalidad de la operación de la plataforma en todos los países miembros, facilitando así una colaboración sin fisuras y respetuosa de las normativas vigentes en cada jurisdicción.

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. Para los usuarios finales, la aplicación proporciona una interfaz web intuitiva y segura. Esta interfaz es el punto de entrada principal para la interacción con el sistema, donde los usuarios pueden autenticarse y acceder a las funcionalidades relevantes de acuerdo con sus roles y permisos. Por otro lado, las aplicaciones internas de los países miembros tienen la capacidad de integrarse directamente con el nuevo sistema a través de APIs robustas y bien documentadas. Estas APIs ofrecen un método programático para realizar operaciones, permitiendo a las aplicaciones automatizar procesos y flujos de trabajo, e interactuar con el sistema central de forma eficiente. Este diseño de doble acceso permite al nuevo sistema ofrecer una solución flexible que se adapta tanto a usuarios individuales que requieren una interfaz gráfica como a sistemas automatizados que necesitan una comunicación directa y programática con el sistema central. Ambos métodos de acceso se benefician de los estándares de seguridad de la información más altos, asegurando la integridad y confidencialidad de los datos manejados dentro del convenio multilateral.

El acceso al entorno completo del nuevo sistema se realiza a través de conexiones seguras HTTPS/TLS, proporcionando un nivel de seguridad esencial tanto para la interfaz de usuario web como para las interacciones de API.

Seguridad en la Interfaz Web: Cuando los usuarios finales acceden al nuevo sistema a través de la interfaz web, HTTPS/TLS actúa como un guardián que encripta la comunicación entre el navegador del usuario y los servidores de la aplicación. Este protocolo de seguridad es vital para proteger la privacidad y la integridad de la información sensible del usuario, como las credenciales de inicio de sesión, los detalles personales y los datos de seguridad social. Al emplear HTTPS/TLS, se asegura que:

- Todos los datos transmitidos están cifrados, lo que significa que incluso si los datos son interceptados durante la transmisión, no pueden ser leídos ni alterados por actores maliciosos.
- La identidad del servidor al que se conectan los usuarios está autenticada, previniendo ataques de intermediarios y asegurando a los usuarios que están comunicándose con el servidor legítimo del nuevo sistema.

- Se establece una conexión segura antes de que se transmita cualquier información, lo que contribuye a la confianza del usuario en la plataforma.

Seguridad en las APIs: Para las aplicaciones de los países miembros que interactúan con el nuevo sistema a través de APIs, HTTPS/TLS es igualmente crucial. Las APIs que están expuestas en la red y son consumidas por sistemas automatizados de países miembros requieren un canal de comunicación que garantice la protección contra la exposición de datos operativos y estratégicos. Con HTTPS/TLS, la aplicación asegura que:

- Las credenciales de API y los tokens de acceso permanecen confidenciales durante la transmisión.
- La integridad de los datos enviados y recibidos a través de las APIs se mantiene, asegurando que las transacciones y las operaciones no sean manipuladas.

Profundizando en la estrategia de seguridad para las APIs, se implementarán técnicas avanzadas de cifrado a nivel de mensaje, abarcando tanto los headers como el payload. Este enfoque, basado en algoritmos criptográficos robustos, establece una barrera adicional para la protección de los datos en tránsito, asegurando que la información sensible permanezca cifrada y segura incluso si se compromete la seguridad del canal HTTPS/TLS. Complementariamente, se exigirá la firma digital de cada mensaje emitido a través de las APIs, para verificar la autenticidad y la integridad de los datos, evitando así manipulaciones y repudio.

La primera etapa en la arquitectura del nuevo sistema es crucial, consistiendo en el acceso al entorno de la aplicación y la autenticación de los usuarios finales y las aplicaciones internas de los países miembros. En este punto, la **gestión de identidades** emerge como un elemento esencial, ya que establece la base de seguridad para todas las interacciones subsiguientes con el sistema. El producto de gestión de identidades es fundamental por varias razones:

- Validación de Identidad: Es el portero inicial que valida las credenciales del usuario o de la aplicación, asegurando que solo las entidades autorizadas puedan acceder al sistema.
- Unificación del Acceso: Proporciona un punto de acceso coherente y seguro, ya sea a través de una interfaz web o mediante una API, lo que es fundamental para mantener un control robusto sobre quién puede ingresar al sistema.

Aquí se resumen las principales funciones y la importancia de este componente:

- Autenticación y Autorización:
    - Centraliza la validación de identidades, ofreciendo un único punto de verdad para la autenticación de usuarios y aplicaciones.
    - Asigna roles y permisos, determinando el nivel de acceso y las operaciones permitidas para cada entidad autenticada teniendo en cuenta el principio de acceso mínimo y los mecanismos de garantía de segregación de funciones y acceso.
- Gestión de Tokens de Acceso:
    - Genera y distribuye tokens seguros tras una autenticación exitosa, que sirven como llaves de acceso temporal para usuarios y aplicaciones.
    - Implementa mecanismos para la revocación y validación de tokens, garantizando que los accesos no autorizados sean rápidamente neutralizados.
- Autenticación Multifactor (MFA):
    - Añade una capa extra de seguridad mediante la verificación de identidad en dos o más pasos, reduciendo significativamente el riesgo de accesos no autorizados.
    - Permite una configuración flexible para adaptarse a diversas necesidades de seguridad y regulaciones específicas.
- Registro y Monitoreo de Actividades: Lleva un registro detallado de todas las acciones realizadas por usuarios y aplicaciones, lo que es vital para la auditoría de seguridad, el cumplimiento normativo y la detección de anomalías.

La interfaz web del nuevo sistema es la puerta de entrada para los usuarios finales, siendo crucial su diseño y funcionalidad para una experiencia de usuario segura y eficiente. A continuación, se detallan los requerimientos y consideraciones tecnológicas para el desarrollo de esta interfaz:

- Requerimientos de Acceso y Usabilidad:
    - Diseño Responsive: La interfaz debe ser accesible y eficiente en una variedad de dispositivos, incluyendo ordenadores, tablets y teléfonos móviles.
    - Navegación Intuitiva: La estructura y navegación de la aplicación web deben ser claras y fáciles de usar para garantizar una experiencia de usuario fluida.
    - Accesibilidad: Implementar soporte para múltiples idiomas, garantizando que usuarios de diferentes regiones puedan interactuar con el sistema en su lengua nativa, además de cumplir con las normativas de accesibilidad web para permitir

que todos los usuarios, incluidos aquellos con discapacidades, puedan manejar la aplicación.

- Seguridad en la Interfaz Web:
    - Cifrado con HTTPS/TLS: Implementar HTTPS para asegurar que toda la comunicación entre el cliente y el servidor esté cifrada y protegida.
    - Defensas contra Ataques Web: Además de medidas estándar de seguridad, se incorporará un Firewall de Aplicaciones Web (WAF) para filtrar y bloquear amenazas dirigidas específicamente a la interfaz web, reforzando la defensa contra vulnerabilidades comunes. Deberá realizarse un análisis de vulnerabilidades y pruebas de penetración a la solución previo a la puesta en producción.
    - Manejo Seguro de Sesiones: Utilizar prácticas seguras en la gestión de sesiones y cookies, incluyendo timeouts de sesión y almacenamiento protegido de tokens.
- Fundamentos Tecnológicos para el Desarrollo:
    - Uso de Frameworks Modernos: Emplear tecnologías de vanguardia como React, Angular.. para la construcción de una interfaz dinámica y mantenible.
    - Estrategias de Optimización Web: Implementar técnicas para mejorar la eficiencia de carga de la página.
    - Pruebas de Compatibilidad y Gestión de Liberaciones Segura: Realizar pruebas exhaustivas en diferentes navegadores y versiones, e integrar prácticas para asegurar un proceso de liberación seguro, permitiendo versiones y retrocesos ágiles y fiables.
    - Operaciones de Healthcheck: Implementar comprobaciones de salud para los servicios expuestos, mejorando así la disponibilidad y el monitoreo del estado del sistema.

El API Gateway en la arquitectura del nuevo sistema actúa como un intermediario crítico que gestiona y dirige el tráfico de entrada tanto de la interfaz web como de las aplicaciones internas de los países miembros hacia los servicios y componentes adecuados de la aplicación. Su papel es vital para facilitar una interacción fluida, segura y eficiente con toda la plataforma. A continuación, se detallan las funciones y el valor que aporta el API Gateway en la arquitectura:

- Enrutamiento de Solicitudes:
    - Intermediario entre Clientes y Servicios: El API Gateway actúa como un punto de entrada único para todas las solicitudes, dirigiéndolas a los microservicios correspondientes.
    - Decomposición de Solicitudes: Capaz de descomponer las solicitudes complejas en múltiples más simples que pueden ser gestionadas de manera eficiente por los servicios de backend.
- Seguridad y Control de Acceso:
    - Autenticación y Autorización: Verifica las credenciales y tokens de acceso, asegurando que solo los usuarios y aplicaciones autorizados puedan acceder a los servicios.
    - Políticas de Seguridad: Implementa políticas de seguridad, como la limitación de tasa y la protección contra ataques comunes, para proteger la aplicación de uso abusivo o malicioso.
- Manejo de APIs:
    - Versionado de APIs: Gestiona diferentes versiones de las APIs para permitir actualizaciones y cambios sin interrumpir los servicios.
    - Aggregación de Servicios: Permite combinar respuestas de múltiples servicios en una única respuesta coherente para el cliente. Además, para garantizar una mayor interoperabilidad y estandarización, se requerirá que el manejo de todas las APIs se realice conforme a los lineamientos de OpenAPI. Esta normativa permitirá una descripción clara y precisa de las interfaces, facilitando su adopción y cumplimiento a través de mecanismos de chequeo automatizados implementados por el API Gateway.
- Mejora del Rendimiento:
    - Caché de Respuestas: Almacena respuestas frecuentes en caché para mejorar la velocidad de respuesta y reducir la carga en los servicios backend. Es crucial que este proceso de caché se diseñe con un enfoque de seguridad integral, garantizando que toda la información sensible almacenada se cifre adecuadamente, manteniendo la coherencia con el esquema de seguridad global que cifra los datos tanto en tránsito como en reposo.
    - Balanceo de Carga: Distribuye las solicitudes entrantes entre instancias de servicios para optimizar el uso de recursos y mejorar el rendimiento.

- Simplificación del Desarrollo de Clientes:
    - Interfaz Única: Proporciona una interfaz única y coherente para los desarrolladores, ocultando la complejidad de los microservicios subyacentes.
    - SDKs y Documentación: Facilita la integración ofreciendo kits de desarrollo de software (SDKs) y documentación detallada para consumir las APIs.

El API Gateway es esencial en la arquitectura del nuevo sistema por su capacidad para gestionar eficazmente el tráfico, aplicar políticas de seguridad, simplificar la interacción con los servicios del backend y mejorar el rendimiento general. Su implementación asegura que tanto la interfaz web como las aplicaciones internas de los países miembros puedan comunicarse de manera segura, eficiente y coherente con la plataforma, contribuyendo significativamente a la escalabilidad, seguridad y mantenibilidad de la aplicación. En la arquitectura del nuevo sistema, se opta por un diseño REST para las APIs dada su naturaleza estandarizada, flexible y eficiente.

El desarrollo de los **servicios de backend** en el nuevo sistema es un componente esencial que sustenta todas las funcionalidades y módulos del sistema. La importancia de diseñar estos servicios radica en su capacidad para procesar, gestionar y almacenar datos de manera eficiente y segura, ofreciendo una base sólida para la operativa general de la aplicación. Para asegurar una arquitectura adaptable y mantenible, los servicios de backend se conceptualizan asociados a diferentes módulos y funcionalidades de la aplicación. Este diseño modular facilita la actualización, escalabilidad y depuración del sistema. En cuanto a los lenguajes de programación, se opta por utilizar tecnologías frecuentes y estándares como Java, JavaScript o Python. Estos lenguajes son ampliamente reconocidos por su robustez, comunidad de soporte y bibliotecas disponibles, lo que los convierte en opciones idóneas para construir servicios de backend fiables y eficientes.

En el desarrollo de los servicios de backend para la aplicación del nuevo sistema, existen dos enfoques predominantes que se consideran para estructurar y desplegar las funcionalidades esenciales del sistema: la arquitectura de microservicios y la arquitectura monolítica. Ambos modelos ofrecen diferentes ventajas y desafíos, y la elección entre uno u otro depende de varios factores incluyendo la complejidad de la aplicación, requisitos de escalabilidad, alta disponibilidad y los recursos disponibles para el desarrollo y mantenimiento. El modelo de microservicios es el enfoque moderno y más alineado con las capacidades de la nube,

caracterizado por dividir la aplicación en un conjunto de servicios más pequeños, independientes y modulares. Cada microservicio se encarga de una parte específica de la funcionalidad de la aplicación y opera de manera autónoma. Este enfoque facilita la escalabilidad, la flexibilidad en el uso de diferentes tecnologías para cada servicio y la capacidad de actualizar o modificar partes de la aplicación sin afectar al resto. Sin embargo, también introduce una mayor complejidad en la coordinación, el monitoreo y la gestión global de los servicios. Por otro lado, la arquitectura monolítica sigue siendo una opción viable y preferida en ciertos contextos. En este modelo, la aplicación se desarrolla como un único y unificado código base. Todos los componentes de la aplicación están interconectados y dependientes entre sí, operando como un único sistema cohesivo. Aunque la escalabilidad y flexibilidad pueden ser limitadas en comparación con los microservicios, la arquitectura monolítica ofrece una simplicidad relativa en el desarrollo, pruebas y despliegue, lo que puede ser especialmente atractivo para aplicaciones con menores requisitos de escalabilidad y complejidad.

Para el nuevo sistema, la evaluación contempla tanto la implementación de una arquitectura de microservicios como la conservación de un enfoque monolítico. Teniendo en cuenta que el volumen de solicitudes gestionadas por la aplicación se anticipa como moderado, y que la naturaleza de las operaciones no exige inherentemente la complejidad de microservicios, el enfoque monolítico surge como una opción pragmática. Este camino no solo simplificaría el desarrollo y la gestión del sistema, sino que también contribuiría a una optimización de costos, alineándose efectivamente con los objetivos de entregar una solución sólida, eficiente y adecuada a las necesidades del proyecto. Si bien la escalabilidad horizontal y la alta disponibilidad son aspectos fundamentales en el diseño de sistemas robustos, en este contexto específico, donde el intercambio de información no demandaría tiempos de respuesta críticos o gestión inmediata, estas características no se presentan como prioritarias. No obstante, aunque el volumen de solicitudes y la inmediatez en la gestión no se destacan como elementos cruciales para la operatividad del nuevo sistema, se adopta un enfoque cauteloso que permite flexibilidad y preparación ante posibles incrementos futuros en la demanda o necesidades operativas, asegurando así la eficacia y seguridad en el intercambio de información a largo plazo.

En la aplicación del nuevo sistema, que gestiona información personal altamente sensible de individuos de diferentes países, la seguridad de los datos es una prioridad máxima. En este

contexto, el producto de **gestión de claves y cifrado** emerge como un componente crítico dentro de la arquitectura de la aplicación, asegurando la protección integral de los datos tanto en tránsito como en reposo en un entorno cloud gestionado por la OISS.

La herramienta para la gestión de claves y el cifrado es fundamentales para proteger los datos almacenados dentro de la aplicación y su infraestructura cloud. El gestor de claves y cifrado se encarga de:

- Cifrar los Datos Almacenados: Asegura que todos los datos sensibles almacenados en bases de datos, sistemas de archivos u otros medios estén cifrados, haciendo inútiles los datos sin las claves de cifrado correctas.
- Administración de Claves: Maneja el ciclo de vida de las claves de cifrado, incluyendo su generación segura, almacenamiento, acceso controlado, rotación periódica y eliminación segura. Esto es vital para mantener la efectividad del cifrado a lo largo del tiempo.
- Auditoría y Control de Acceso: Ofrece mecanismos para auditar el uso de las claves de cifrado y controlar quién tiene acceso a ellas. Esto no solo contribuye a la seguridad sino también al cumplimiento normativo, asegurando que solo personal autorizado tenga acceso a las claves y a los datos cifrados.

El gestor de claves y cifrado en reposo es esencial en un entorno cloud donde la infraestructura física es gestionada por un tercero (en este caso, la OISS). Asegura que, incluso si los mecanismos de seguridad perimetrales son vulnerados o hay un acceso no autorizado al entorno de almacenamiento, los datos permanezcan seguros y protegidos. En conjunto, el cifrado en tránsito a través de HTTPS/TLS y la gestión de claves y cifrado en reposo forman un escudo robusto alrededor de la información manejada por el nuevo sistema, manteniendo los estándares más altos de seguridad y cumpliendo con las normativas internacionales de protección de datos.

En la arquitectura del nuevo sistema, los requerimientos de almacenamiento son una consideración primordial debido a la naturaleza y el volumen de los datos manejados, incluyendo información personal y documentos asociados a las solicitudes de seguridad social. Para satisfacer estas necesidades, la aplicación debe contar con sistemas robustos y seguros tanto para el almacenamiento de datos estructurados como para documentos y archivos.

Para el almacenamiento de datos estructurados, se requiere una base de datos que ofrezca confiabilidad, rendimiento y características de seguridad avanzadas para proteger la información sensible. Aunque existen múltiples sistemas de gestión de bases de datos, para una aplicación como el nuevo sistema, donde se prioriza la estabilidad y la facilidad de mantenimiento, las bases de datos SQL son una opción adecuada. Estas bases de datos no solo son ampliamente utilizadas y soportadas, sino que también proporcionan un modelo bien establecido y comprendido para el manejo de datos. Las alternativas en este ámbito podrían incluir sistemas ampliamente reconocidos y probados como MySql, PostgreSQL…

Para el almacenamiento de documentos y archivos, como imágenes o documentos PDF asociados a las solicitudes, se necesita un gestor de archivos que sea capaz de almacenar, indexar y recuperar eficientemente este tipo de datos. Este sistema debe ser seguro, permitiendo el cifrado de los archivos almacenados y asegurando que solo usuarios autorizados puedan acceder a ellos. Además, debe ser capaz de integrarse de manera eficiente con el resto de la arquitectura de la aplicación y soportar una gestión básica de documentos sin requerir las capacidades completas de un sistema de gestión documental avanzado, lo que podría resultar en una solución más compleja y costosa de lo necesario para los requerimientos del nuevo sistema.

Ambos sistemas de almacenamiento, tanto para datos estructurados como para documentos, deben ser gestionados y soportados por el proveedor cloud, aprovechando las ventajas en términos de escalabilidad, disponibilidad y seguridad.

El proveedor adjudicatario deberá entregar una documentación técnica exhaustiva y guías de usuario detalladas para el Nuevo Sistema, asegurando una comprensión integral de su infraestructura y funcionalidades. Esta documentación incluirá manuales técnicos para la configuración y mantenimiento, así como guías paso a paso para los usuarios finales, facilitando la navegación y el aprovechamiento de todas las características del sistema. Adicionalmente, se espera que el proveedor ofrezca capacitaciones dirigidas a los administradores y usuarios, proporcionando las habilidades necesarias para un uso eficiente y seguro del Nuevo Sistema.

DESCRIPCIÓN DE LOS MÓDULOS FUNCIONALES DE LA APLICACIÓN

En esta sección del informe, nos adentramos en la descripción funcional del nuevo sistema, delineando cómo sus distintos componentes trabajan conjuntamente para gestionar y facilitar el intercambio de información entre países. El nuevo sistema se plantea con un diseño modular, en el que cada módulo es una unidad independiente centrada en una funcionalidad específica, pero al mismo tiempo, está diseñado para integrarse armoniosamente con el resto de la plataforma, asegurando un sistema cohesivo y eficiente. En los siguientes apartados, exploraremos más a fondo cada uno de estos módulos funcionales, entendiendo su contribución única al conjunto de la aplicación.

Modulo gestión de usuarios

El módulo de Gestión de Usuarios desempeña un papel crucial al proporcionar una estructura organizada y segura para el manejo de las cuentas de usuario. En este marco, la OISS actúa como administrador principal de la aplicación, asumiendo la responsabilidad inicial de gestionar el alta de los administradores delegados por cada país. Esta responsabilidad incluye asegurar que los administradores asignados posean las credenciales y autorizaciones necesarias para llevar a cabo su función dentro de la plataforma. Una vez establecidos, los administradores delegados por país toman la responsabilidad de gestionar los usuarios dentro de su jurisdicción. Este proceso incluye:

- **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. Esto incluye la activación, actualización, suspensión y eliminación de cuentas de usuario, asegurando que solo personal autorizado tenga acceso a la información y funcionalidades de sistema.
- **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. Esta asignación de roles es gestionada de manera local por los administradores delegados, permitiendo una adaptación más precisa a las necesidades y estructuras de cada país.

- **Ciclo de Vida de los Usuarios:** Es fundamental una gestión activa del ciclo de vida de los usuarios, que abarca desde su creación hasta su eventual baja del sistema. Esto incluye la actualización periódica de permisos, la reasignación de roles según las necesidades cambiantes, y la desactivación o eliminación de usuarios que ya no requieren acceso a la plataforma.

La propuesta de una administración delegada por país tiene como objetivo principal garantizar que la gestión de usuarios sea lo más cercana y adaptada posible a las particularidades de cada sistema de seguridad social nacional. Los administradores delegados son responsables de validar la identidad y elegibilidad de los usuarios dentro de su jurisdicción, asegurando una gestión precisa y segura de accesos. Esta estructura no solo permite una gestión descentralizada y eficiente, sino que también promueve la responsabilidad y autonomía de cada país en la gestión de su personal, asegurando que la plataforma cumpla con las diversas regulaciones y prácticas locales.

Modulo gestión de formularios

El módulo de Gestión de Formularios se centra en la parametrización y administración de los formularios requeridos para las diferentes solicitudes de intercambio de información. La validación y otras operaciones complejas se manejan en otro módulo dedicado, manteniendo así una separación clara de responsabilidades dentro de la arquitectura de la aplicación. Aspectos fundamentales del módulo de Gestión de Formularios incluyen:

- **Parametrización y Flexibilidad:** Los administradores pueden definir y modificar la estructura de los formularios, incluyendo campos, tipos de datos y opciones disponibles, adaptando la aplicación a los requerimientos específicos de cada tipo de solicitud y a los cambios normativos. Esta flexibilidad asegura que el nuevo sistema pueda responder rápidamente a las necesidades emergentes o modificaciones en los estándares internacionales.
- **Relación con Roles de Usuario:** La gestión de formularios está intrínsecamente ligada a los roles definidos en el módulo de Gestión de Usuarios. Dependiendo del rol asignado, un usuario tendrá permisos para crear, modificar, enviar o realizar otras acciones sobre los formularios. Esta integración asegura que las operaciones en los formularios se realicen siempre dentro del marco de seguridad y permisos adecuados.
- **Gestión de Documentos Adjuntos:** Entendiendo que los procedimientos de seguridad social frecuentemente requieren la presentación de documentación adicional, el módulo

facilita la asociación y manejo de documentos adjuntos. Los usuarios pueden cargar, gestionar y adjuntar fácilmente los documentos necesarios a sus formularios.

- **Configuración y Adaptación Continua:** El módulo permite una actualización y configuración continua de los formularios para reflejar cambios legislativos, políticas específicas de países o mejoras en los procesos. La capacidad de adaptarse y configurarse de manera dinámica es crucial para el mantenimiento de la relevancia y efectividad de la plataforma.

Modulo gestión de validaciones

El módulo de Gestión de Validaciones es fundamental para mantener la integridad y precisión de toda la información procesada y compartida en la plataforma. Este módulo, trabajando en sinergia con el módulo de Gestión de Formularios, se encarga de la validación tanto de datos estructurados ingresados en los formularios como de los datos no estructurados, tales como documentos e imágenes que se adjuntan a las solicitudes. Las funciones principales de la Gestión de Validaciones incluyen:

- **Validación de Datos Estructurados:** Define y aplica reglas dinámicas para la validación de campos específicos en los formularios. Esto incluye la comprobación de formatos, rangos, consistencia lógica y cualquier otro criterio necesario para asegurar la exactitud de los datos capturados.
- **Validación de Datos No Estructurados:** Extiende la capacidad de validación a documentos y archivos adjuntos, asegurando que los documentos subidos cumplen con los requisitos de formato, tamaño y tipo especificados. También puede incluir la **comprobación de la legibilidad o relevancia del contenido donde sea aplicable.**
- Validación de Seguridad de Documentos y Archivos Adjuntos: Antes del almacenamiento, se realiza una inspección de seguridad para verificar que los documentos y archivos adjuntos estén libres de virus o malware. Esta validación preventiva asegura la subida de archivos seguros y confiables, protegiendo el sistema contra la introducción de software malicioso.
- **Reglas de Validación Configurables:** Permite a los administradores configurar y actualizar las reglas de validación para adaptarse a los cambios en los requerimientos legales, políticas internacionales o simplemente para mejorar la calidad del proceso de intercambio de datos.

- **Retroalimentación y Corrección:** Ofrece a los usuarios retroalimentación inmediata sobre los errores o inconsistencias encontrados durante la validación, con sugerencias claras para su corrección. Esto facilita un proceso interactivo donde los usuarios pueden corregir y mejorar la calidad de los datos antes de su envío final.
- **Registro y Auditoría:** Mantiene un historial completo de todas las validaciones realizadas, incluyendo los errores detectados y las acciones de corrección tomadas. Esto es vital para procesos de auditoría, control de calidad y para la mejora continua del sistema de validación.

Módulo gestión de notificaciones

El módulo de Gestión de Notificaciones es una herramienta esencial que asegura la comunicación efectiva y oportuna con los usuarios de la plataforma. Este módulo se encarga de enviar notificaciones automáticas relacionadas con las nuevas solicitudes ingresadas, así como los cambios de estado y actualizaciones relevantes en el ciclo de vida de cada solicitud. La capacidad de configuración y parametrización de las notificaciones permite una adaptabilidad significativa, asegurando que la información llegue a los usuarios correctos en el momento adecuado. Las características principales del módulo de Gestión de Notificaciones incluyen:

- **Notificaciones Automatizadas:** El sistema envía automáticamente notificaciones a los usuarios pertinentes basadas en eventos específicos dentro de la aplicación, como la incorporación de nuevas solicitudes o cambios en el estado de las mismas.
- **Configuración de Notificaciones:** Los administradores pueden configurar y parametrizar el tipo, el contenido y el momento de las notificaciones. Esto permite adaptar las comunicaciones a las necesidades específicas de diferentes grupos de usuarios o tipos de solicitudes.
- **Personalización de Mensajes:** Los mensajes de notificación pueden ser personalizados para incluir información relevante y específica relacionada con la solicitud o el usuario, mejorando la claridad y efectividad de la comunicación.
- **Diversos Canales de Comunicación:** Las notificaciones pueden ser enviadas a través de diversos canales, como correo electrónico, mensajes de texto, o incluso integraciones con sistemas internos de los países miembros, asegurando que se adapten a las preferencias y requisitos de los usuarios.

- **Seguimiento de Notificaciones:** El módulo permite un seguimiento de las notificaciones enviadas, incluyendo detalles sobre la entrega y recepción de los mensajes, así como la capacidad de reenviar o ajustar notificaciones si es necesario.

Módulo gestión de estados

El módulo de Gestión de Estados es vital para el adecuado seguimiento y control del ciclo de vida de cada solicitud que se maneja en la plataforma. Este módulo permite definir y gestionar los distintos estados por los que una solicitud puede transitar, desde su creación hasta su conclusión, y vincular estos estados con las acciones permitidas, las validaciones necesarias y las notificaciones correspondientes. Características clave del módulo de Gestión de Estados:

- **Definición de Estados:** Administradores pueden definir una serie de estados a través de los cuales transitan las solicitudes, tales como "Pendiente de Validación", "En Revisión", "Aprobada", "Rechazada", etc. Cada estado refleja una etapa específica en el ciclo de vida de la solicitud.
- **Transiciones y Reglas:** Establece reglas y transiciones entre estados, definiendo qué acciones deben ocurrir para que una solicitud pase de un estado a otro. Esto incluye la configuración de eventos automáticos o acciones requeridas por parte de los usuarios.
- **Asociación con Acciones y Roles:** Cada estado puede estar asociado con acciones específicas que diferentes roles de usuario pueden o no pueden realizar. Por ejemplo, solo ciertos roles pueden aprobar o rechazar solicitudes, mientras que otros pueden solo visualizarlas o agregar información. Adicionalmente, se podrán implementar acciones automáticas asociadas a diferentes estados, como la de eliminar la información depositada en las bases de datos de la aplicación en la nube cuando la solicitud se encuentre ya gestionada y finalizada.
- **Integración con Notificaciones:** El módulo está integrado con el sistema de Gestión de Notificaciones para enviar alertas automáticas cada vez que una solicitud cambia de estado, asegurando que los usuarios pertinentes estén informados sobre el progreso o la necesidad de acción.
- **Auditoría y Seguimiento:** Proporciona capacidades de auditoría y seguimiento, permitiendo a los administradores y usuarios ver el historial completo de estados por los que ha pasado cada solicitud, incluyendo cuándo y quién hizo cambios en el estado.

Modulo gestión de informes

El módulo de Gestión de Informes es una herramienta clave para la monitorización y análisis del desempeño de la plataforma, proporcionando información valiosa para la toma de decisiones y la mejora continua. Este módulo se encarga de generar informes y estadísticas detalladas sobre la gestión de las solicitudes, los tiempos de procesamiento, los estados de las solicitudes, entre otros indicadores relevantes. Este módulo de Gestión de Informes se contará con capacidades avanzadas de auditoría, esenciales para garantizar una trazabilidad completa y robusta de las acciones realizadas en el sistema. Estas capacidades incluyen:

- **Trazas de Auditoría para la Gestión de Perfiles y Usuarios:** Permite la generación de registros detallados que documentan todas las acciones realizadas en la gestión de perfiles y usuarios, desde la creación, modificación, hasta la desactivación o eliminación de cuentas. Esto asegura una visibilidad completa sobre quién hizo qué, cuándo y desde dónde, facilitando la revisión y el control de las actividades administrativas.
- **Auditoría de Acceso de Usuarios:** Proporciona información detallada sobre el acceso de los usuarios al sistema, incluyendo intentos de inicio de sesión exitosos y fallidos, cambios de contraseña, y otras acciones relevantes al acceso y seguridad de las cuentas. Esta función es crucial para detectar y responder a actividades sospechosas o no autorizadas.
- **Monitoreo de Actividades y Consultas de Datos:** Abarca la generación de trazas de auditoría para todas las consultas de datos realizadas dentro del sistema, asegurando que cualquier acceso a los datos, ya sea para consulta, modificación o eliminación, quede registrado. Este nivel de detalle es fundamental para cumplir con las normativas de protección de datos y para realizar análisis forenses en caso de incidentes de seguridad.

Aspectos fundamentales del módulo de Gestión de Informes:

- **Generación de Informes:** Permite la creación de informes dinámicos que reflejan distintos aspectos de la gestión de la plataforma, como el volumen de solicitudes, los tiempos de procesamiento promedio, las tasas de aprobación/rechazo y otros indicadores de rendimiento.
- **Desagregación de Datos:** Ofrece la capacidad de desglosar la información según varios criterios, como tipo de solicitud, país, período de tiempo, entre otros, permitiendo análisis específicos y detallados.

- **Exportación de Datos:** Los usuarios con los permisos adecuados pueden exportar datos e informes según necesiten, en diferentes formatos, para su análisis o presentación externa. Esto facilita la integración de los datos del nuevo sistema con otros sistemas o procesos de reporte.
- **Protección de la Información Personal:** Aunque el módulo gestiona y procesa grandes volúmenes de datos, se asegura que toda la información personal esté disociada o protegida, en línea con las regulaciones de protección de datos. Solo la información necesaria y no sensible permanece en la base de datos de la aplicación cloud de forma permanente.
- **Asociación con Roles y Permisos:** El acceso a los informes y datos estadísticos está estrictamente controlado y es asignado según los roles y permisos de los usuarios. Esto asegura que solo personal autorizado pueda acceder a esta información, manteniendo la seguridad y privacidad de los datos.
- **Visualización e Interpretación:** Incluye herramientas de visualización para facilitar la interpretación de los datos, como gráficos, tablas y otras representaciones gráficas que ayudan a comprender las tendencias y patrones en la gestión de las solicitudes.