Subsecretaría de Previsión Social

Ficha Única de Información Laboral y Previsional

Informe de Diseño

Febrero 2025

INTRODUCCIÓN

Este informe presenta el diseño de la Ficha Única de Información Laboral y Previsional, una herramienta clave para mejorar la interoperabilidad entre los Órganos de la Administración del Estado (OAEs) del Ministerio del Trabajo y Previsión Social. La propuesta busca optimizar la gestión de datos mediante un modelo centralizado que permita la colaboración interinstitucional eficiente, reduciendo redundancias y fortaleciendo los procedimientos administrativos bajo estrictos estándares de seguridad y cumplimiento normativo.

El documento establece como eje técnico la creación de un Nodo Laboral y Sectorial, diseñado para centralizar el intercambio de datos transaccionales entre las instituciones y garantizar un manejo seguro y trazable de la información. Este nodo, interconectado con la Plataforma Integrada de Servicios Electrónicos del Estado (PISEE 2.0), redefine los convenios tradicionales hacia un enfoque sectorial, permitiendo que los datos se compartan de manera estandarizada y accesible para las entidades involucradas.

Para sustentar esta propuesta, se define una arquitectura basada en cinco principios fundamentales: centralización sectorial, interoperabilidad, coreografía de procesos, escalabilidad y cumplimiento normativo. Este marco técnico no solo habilita la gestión eficiente de las transacciones, sino que también aborda desafíos clave como la infraestructura necesaria, los riesgos asociados y las estrategias de seguridad. Se identifican componentes críticos como la implementación de servidores robustos, redes de alta disponibilidad y mecanismos avanzados de control de acceso, diseñados para garantizar la confiabilidad y la continuidad operativa del sistema.

Por último, se recomienda un plan de implementación que permite iniciar con la marcha blanca de la infraestructura en los primeros 6 meses de implementación, evolucionando durante los siguientes 12 meses el sistema a un nivel sectorial y totalmente interoperable.

TABLA DE CONTENIDOS

1. Antecedentes generales

1.1. Transformación Digital

La transformación digital ha emergido como un eje central para la modernización de los gobiernos, redefiniendo la forma en que las instituciones públicas operan, interactúan y entregan valor a la ciudadanía. Más allá de la adopción de tecnología, este proceso implica una transformación sistémica que abarca tres pilares fundamentales: personas e instituciones, procesos y tecnología.

Estos pilares no actúan de manera aislada, sino que forman un sistema interdependiente que debe ser abordado estratégicamente. Es decir, deben evolucionar en conjunto para asegurar una transformación efectiva y sostenible.

1.1.1. Personas e Instituciones

El componente humano de la transformación digital aborda dos perspectivas: los ciudadanos como benefactores finales de los servicios públicos y los funcionarios públicos como operadores y gestores de las plataformas digitales. La digitalización de los servicios públicos tiene una relación directa con ambos grupos, impactando en la manera en que interactúan con el Estado y acceden a los beneficios de una administración más eficiente.

1. **Usuarios finales (ciudadanos y empresas)**:

   La digitalización tiene como objetivo eliminar las barreras físicas y administrativas, facilitando el acceso a los servicios del Estado de manera simplificada. Esto responde a la necesidad de los ciudadanos de contar con servicios rápidos, eficaces y proactivos, asegurando que las instituciones públicas estén preparadas para atender de manera ágil y eficiente las demandas.

   En Chile, esto se ha materializado en algunas iniciativas, como la implementación de **Clave Única**, una plataforma que permite la autenticación segura y estandarizada de los ciudadanos para acceder a servicios digitales en múltiples instituciones del Estado, contando actualmente con más de 15 millones de usuarios activos[1]. Además, la migración del 87% de los trámites a formatos digitales refleja el compromiso del Estado chileno con la simplificación de procedimientos[2], asegurando que los servicios sean accesibles de manera remota.

2. **Funcionarios públicos**:

   El éxito de la transformación digital depende también de la capacidad de los funcionarios para adaptarse y gestionar el cambio. En Chile, los **coordinadores de transformación digital** han sido designados como puntos de enlace clave dentro de las instituciones públicas, asumiendo responsabilidades como la implementación de

[1] Estadística entregada en sitio de Gobierno Digital en pestaña *Clave Única*
[2] Estadística entregada en sitio de Gobierno Digital en pestaña *Trámites*

plataformas interoperables, la facilitación de comunicaciones internas y la promoción de estándares técnicos comunes

3. **Órganos de la Administración del Estado (OAE)**

   Dentro del proceso de transformación digital, los OAE actúan como proveedores y consumidores de los servicios de interoperabilidad, mediante los cuales intercambian datos, documentos y expedientes electrónicos entre ellos, permitiendo mantener trazabilidad sobre las acciones ejecutadas entre OAEs, de forma automatizada.

   Para ejecutar estas labores, se requiere que el traspaso de información se dé formal y rápidamente, para que las OAEs puedan cumplir con sus responsabilidades y atender las necesidades de la ciudadanía, manteniendo las normativas de intercambio de información, sin que esto signifique una carga adicional a su labor.

1.1.2. Procesos

Un proceso es un conjunto estructurado de actividades interrelacionadas que transforman elementos de entrada en resultados específicos, a partir del uso de recursos definidos y operando bajo regulaciones establecidas. Estos componentes trabajan de manera coordinada para alcanzar metas organizacionales específicas, permitiendo a las instituciones realizar sus labores de manera eficiente y efectiva.

La transformación digital del Estado requiere una revisión y rediseño integral de los procesos institucionales o procedimientos administrativos para alinearlos con los objetivos estratégicos establecidos. Esta modernización no solo optimiza recursos, sino que además, mediante, la digitalización y automatización, libera tiempo valioso que puede destinarse hacia actividades de mayor impacto. Un elemento fundamental en esta transformación es la adopción de un enfoque centrado en el ciudadano, garantizando que los servicios y productos desarrollados respondan efectivamente a sus necesidades, elevando así los niveles de satisfacción y mejorando la experiencia general.

En este contexto, resulta necesario implementar no solo sistemas internos que faciliten la comunicación organizacional, sino también establecer mecanismos de interoperabilidad robustos entre diferentes áreas, plataformas e instituciones, fomentando una comunicación más fluida y eficiente, tanto dentro de cada organización como en la interacción entre distintas entidades públicas.

Actualmente, esta responsabilidad recae sobre cada OAE, quienes deben adecuar sus sistemas para cumplir con los estándares de transformación digital exigidos en los plazos correspondientes según la normativa[3].

[3] Plazos estipulados en el Decreto con Fuerza de Ley Nº1 por parte del Ministerio Secretaría General de la Presidencia en 2020, modificados en 2022 por la Ley Nº21.464.

1.1.3. TECNOLOGÍA

Por último, la tecnología desempeña un rol central como habilitador principal de la transformación digital, proporcionando las herramientas necesarias para integrar y escalar los diferentes elementos del sistema organizacional.
En Chile, la interoperabilidad se apoya en soluciones tecnológicas clave, como el PISEE[4], diseñada para habilitar la interoperabilidad entre OAEs.

Para garantizar la interacción eficiente entre los sistemas gubernamentales, se han implementado estándares abiertos y APIs que permiten el intercambio de datos en tiempo real entre distintas instituciones. Este enfoque asegura que la información compartida sea consistente y accesible, además de reducir las redundancias en los registros y mejorando la coordinación interinstitucional, promoviendo una operación más integrada y colaborativa.
Además, la protección de la información se ha consolidado como un pilar fundamental en la transformación digital del Estado, manifestándose en dos aspectos cruciales.

- La incorporación de medidas avanzadas de ciberseguridad en las plataformas implementadas, alineadas con normativas técnicas específicas para prevenir accesos no autorizados.
- El marco regulatorio, fortalecido por la Ley de Protección de Datos Personales y la creación de la Agencia de Protección de Datos Personales, establece responsabilidades claras para entidades públicas y privadas en el manejo de información personal.

Esta estructura busca garantizar la privacidad y el derecho a la autodeterminación informativa de los ciudadanos, reforzando la confianza en el ecosistema digital, asegurando su sostenibilidad a largo plazo y protegiendo a la ciudadanía frente al uso indebido o no autorizado de sus datos.

1.2. LEY DE TRANSFORMACIÓN DIGITAL

Los avances y lineamientos descritos anteriormente forman parte de la estrategia establecida en la Ley N°21.180 de Transformación Digital del Estado promulgada en 2019, cuyo propósito fundamental es modernizar la administración pública mediante la digitalización de trámites y procedimientos institucionales.

Con esta legislación se busca evolucionar hacia un modelo que simplifique la experiencia de los ciudadanos, potencie la coordinación interinstitucional y optimice los tiempos de atención y respuesta, promoviendo una administración más dinámica y efectiva. El enfoque central de esta transformación sitúa las necesidades ciudadanas como eje principal de la gestión pública, garantizando un servicio más eficiente y orientado al usuario.

[4] Plataforma PISEE con el catálogo de servicios (fuentes de datos) ofrecidos actualmente por algunos OAEs. Para mayor entendimiento, se comparte la guía de esta solución de interoperabilidad.

Bajo este contexto, se definen seis fases que marcan la hoja de ruta asociada al proceso hasta su total implementación en 2027, dentro de las que se encuentran:

- **Comunicaciones oficiales:** Las comunicaciones oficiales entre órganos serán registradas en plataforma destinada a este fin.
- **Inicio de procedimientos administrativos en forma digital:** Cada órgano deberá establecer plataformas o formularios electrónicos para que las personas puedan realizar el ingreso de solicitudes o documentos al Estado.
- **Expedientes electrónicos:** Para fortalecer la transparencia de los procesos, cada procedimiento administrativo contará con expedientes electrónicos, disponibles para los interesados/as a través de plataformas electrónicas
- **Digitalización del documento en papel:** En caso de que una persona esté imposibilitada del uso de medios electrónicos, el órgano correspondiente deberá digitalizar e ingresar al expediente electrónico sus solicitudes.
- **Principio de interoperabilidad:** Los órganos deberán cumplir con el principio de interoperabilidad, es decir, que los medios electrónicos sean capaces de interactuar y operar entre sí al interior de la Administración del Estado, a través de estándares abiertos para una interconexión segura y expedita.
- **Notificaciones electrónicas:** Las notificaciones a personas naturales o jurídicas se practicarán por medios electrónicos en base a la información contenida en un registro único dependiente del Servicio de Registro Civil.

Para lograr el avance de este proceso, se han definido estándares y directrices técnicas que los diferentes OAEs deben cumplir para implementar la ley. Dentro de estos se encuentran:

- **Intercambio de documentos electrónicos (interoperabilidad)**: deberán utilizar sistemas integrados de conexiones directas y seguras a través de internet, operando mediante nodos alojados en la infraestructura informática de los órganos estatales, que permita a las instituciones actuar como proveedores y/o consumidores, que intercambien eficientemente datos, documentos y expedientes electrónicos a través de plataformas especializadas (PISEE).

- **Seguridad de la información y ciberseguridad**: los órganos del Estado deberán resguardar la confidencialidad, integridad, disponibilidad de la información y la infraestructura informática, de las plataformas electrónicas que sustentan sus procedimientos administrativos.

- **Documentos y Expedientes Electrónicos**: la administración y gestión de los documentos y expedientes electrónicos debe seguir estándares, formatos, metadatos, registros de trazabilidad, fases y procesos que obren en poder de los OEA a raíz de la tramitación de un procedimiento administrativo. (Simple / gestor documental)

- **Notificaciones**: se aplicará un mecanismo uniforme para las comunicaciones electrónicas entre los órganos de la Administración del Estado y los ciudadanos, en base a un registro único que facilita y estandariza el proceso de notificación en los procedimientos administrativos.

- **Calidad y Funcionamiento**: deberán implementar medidas para garantizar la continuidad operacional y prevenir la obsolescencia tecnológica de las plataformas. Esto incluye el establecimiento de niveles óptimos de servicio, sistemas de monitoreo continuo, soporte técnico y mecanismos para aumentar la resiliencia tecnológica, asegurando el funcionamiento óptimo de las plataformas que sustentan los procedimientos administrativos.

1.3. Desafíos y Oportunidades

La implementación de la estrategia de transformación digital cambiará de manera significativa la forma en que el Estado administra sus procesos. Aunque los avances logrados hasta ahora han evidenciado un progreso importante, también han puesto de manifiesto desafíos que limitan su eficiencia. Estos retos, a su vez, generan oportunidades para mejorar y consolidar el camino hacia los objetivos planteados en la modernización digital.

1.3.1. Desafíos

La transformación digital del Estado enfrenta diversos obstáculos que dificultan su consolidación. Estos desafíos surgen, principalmente, por la falta de coordinación entre las instituciones y la ausencia de mecanismos que garanticen un intercambio de información fluido y consistente. En consecuencia, la ciudadanía y los funcionarios se ven afectados por la lentitud, la duplicación de trámites y la sobrecarga administrativa. A continuación, se presentan los principales ámbitos en los que estas deficiencias se manifiestan con mayor claridad:

- **Interoperabilidad:** Las instituciones han modernizado sus procesos de manera independiente, generando un mosaico de sistemas y normas internas que dificulta la comunicación entre ellas. Esta dispersión incrementa la burocracia y prolonga los tiempos de respuesta.
- **Notificaciones Electrónicas:** Aunque se está desarrollando una herramienta para informar al ciudadano, como el Domicilio Digital Único, esta se concentra en el vínculo entre la Administración y el ciudadano. Se ha dejado de lado la notificación interinstitucional, limitando la posibilidad de que la información circule con fluidez entre los distintos OAE.
- **Fragmentación Administrativa:** La falta de una visión global y coordinada obliga a la ciudadanía a entregar reiteradamente la misma información a distintas instituciones para completar un solo trámite, o actuar de intermediario entre estas entregando la información distribuida entre las OAEs con el mismo fin. Este círculo vicioso, además de resultar en un desgaste para el usuario, genera una alta carga de trabajo manual para los funcionarios responsables de validar los datos una y otra vez.

Esta estructura inicial ofrece una visión general, seguida de una presentación ordenada de los problemas más críticos, lo que hace más sencillo comprender el escenario completo y las áreas específicas en las que es necesario intervenir.

1.3.2. OPORTUNIDADES

La superación de los desafíos identificados exige una evolución en el modelo de interacción entre las instituciones públicas. Hasta ahora, el enfoque dominante ha sido individual, donde cada una ha adecuado sus sistemas y procedimientos administrativos. Esta lógica, si bien resulta útil para comenzar el proceso, termina limitando la autonomía, flexibilidad y escalabilidad necesarias para alcanzar un nivel superior de integración.

Para lograr una interoperabilidad más ágil, surge la propuesta de adoptar un modelo donde las distintas instituciones pueden actuar con mayor independencia, siguiendo lineamientos comunes que favorecen la colaboración sin depender de una entidad central que dicte todos los pasos. Este cambio de paradigma abre la puerta a un entorno más dinámico, en el que las entidades estatales se comuniquen de forma directa, coordinada y fluida.

En este escenario, se identifican tres direcciones de cambio que, combinadas, ofrecen oportunidades significativas para modernizar la gestión pública:

- **Mantención Consolidada de Estados:** Establecer una plataforma centralizada para visualizar y monitorear el estado de los procedimientos administrativos en tiempo real. Este enfoque facilita el seguimiento, reduce la duplicidad de esfuerzos y asegura que cada institución pueda acceder a información actualizada, mejorando así la coherencia y el control sobre los procesos.
- **Integración de Procesos Conexos:** Vincular procedimientos administrativos que se inician en una institución pero influyen en otras, generando flujos de trabajo integrados y sin fisuras. A su vez, esto permite tener una visión global de los datos del sector, haciendo posible la utilización de estos para la mejora de sus servicios, evitando tareas redundantes y acelerando la circulación de información, logrando optimizar la respuesta hacia la ciudadanía y liberar recursos para labores de mayor valor público.
- **Coordinación Interinstitucional mediante Pub/Sub (Publicación/Suscripción):** Inspirado en arquitecturas tecnológicas distribuidas, el uso de un sistema de publicación y suscripción (Pub/Sub) permite a las instituciones “publicar” información relevante y, a su vez, “suscribirse” a la información proveniente de otras entidades. En lugar de una orquestación centralizada, este modelo de “coreografía informativa” asegura que cada participante reciba las actualizaciones necesarias sin necesidad de solicitudes puntuales entre organismos. Este sistema de notificaciones estándar y trazable registra cada intercambio, generando transparencia, accountability y una mejor disposición para la toma de decisiones.

Considerando este conjunto de oportunidades, el sistema proporcionará una visión general de los datos y servicios disponibles en el sector, permitiendo a cada OAE no solo acceder y utilizar información tradicional para sus trámites, sino también identificar oportunidades para integrar otros recursos que puedan mejorar sus servicios y procesos internos.

2. Objetivos del Proyecto

2.1. Objetivo general

En respuesta a los desafíos y oportunidades comentados, se busca diseñar una solución sectorial que centralice la información laboral y previsional de 11 instituciones pertenecientes al sector del Trabajo y Previsión Social. Esta iniciativa se materializará en una Ficha Única, que integrará eficientemente los datos en la red de interoperabilidad del Estado, permitiendo su acceso tanto por parte de las instituciones como de la ciudadanía.

El objetivo principal de la Ficha Única de Información Laboral y Previsional es entregar un consolidado estructurado de la información de datos y servicios provistos por las OAEs del sector trabajo y previsión social. Por otro lado, se busca establecer un Nodo Sectorial que permita la interoperabilidad de los datos y servicios que nutrirán la ficha. Este mecanismo busca mejorar los procesos internos de las instituciones participantes y facilitar a la ciudadanía el acceso a la información necesaria para el ejercicio de sus derechos y deberes.

Para establecer las definiciones necesarias que permitan cumplir con los objetivos explicados anteriormente, se realizan reuniones semanales entre los equipos consultor y Contraparte SPS y con las OAEs pertenecientes a la solución inicial.

2.2. Objetivos específicos

Los objetivos específicos de la Ficha Única de Información Laboral y Previsional son:

1. Canalizar la oferta y demanda de datos entre las 11 instituciones participantes apuntando a las funciones propias de cada una de ellas (fiscalización, entrega de beneficios, decisiones de política pública, estudios).
2. Disponer interactivamente datos consolidados, que sean de interés para la ciudadanía, que sean de relevancia para sus transacciones o servicios en línea; y generar una oferta de valor respecto de la información que se pone a disposición (de manera customizada)

En cambio, **los del Nodo Sectorial laboral y Previsional son:**

1. **Diseñar la interoperabilidad sectorial**: Diseñar un modelo estandarizado que permita la oferta y puesta a disposición de información relevante del sector Trabajo y Previsión Social, bajo la perspectiva de interoperabilidad sectorial.
2. **Diseñar un sistema inteligente de gestión de datos**: Crear un modelo eficiente para la recolección, resguardo y sistematización de la información dentro del Ministerio, asegurando su disponibilidad y precisión para diversas necesidades operativas y estratégicas.
3. **Disposición estandarizada de la información**: Garantizar que los datos sean accesibles de manera oportuna y confiable a:
    - Instituciones, para la ejecución eficaz de sus funciones.
    - Ciudadanos, para la consulta de antecedentes y realización de trámites.
    - El Estado, para la mejora en la oferta de servicios públicos y toma de decisiones informadas.

Estos objetivos buscan consolidar una herramienta centralizada que facilite el intercambio de información, optimizando la atención ciudadana y la eficiencia institucional.

3. PROPUESTA DE INTEROPERABILIDAD

3.1. PRINCIPALES ELEMENTOS DEL SISTEMA PROPUESTO DE INTEROPERABILIDAD

Los siguientes elementos constituyen la base técnica sobre la cual se implementará la solución de la Ficha Única y el nodo sectorial. Estos componentes permiten a las instituciones intercambiar información, sincronizar trámites y adaptarse a distintas necesidades sin requerir un control centralizado en cada etapa.

- **PISEE 2.0:** Este componente es fundamental para el sistema propuesto, pues posibilita el intercambio seguro y eficiente de datos, documentos y expedientes entre instituciones públicas. Su arquitectura combina nodos de interoperabilidad con servicios centralizados, posibilitando flujos independientes y ágiles. Integra herramientas clave para la gestión de información (Catálogo de Servicios, Registro de Trazabilidad, Directorio de Datos, Catálogo de Esquemas, Gestor de Autorizaciones y Gestor de Acuerdos), así como módulos para validación de identidad, coordinación de comunicaciones y monitoreo del sistema.
- **Instituciones involucradas:** El proyecto contempla la participación de 11 instituciones del sector Trabajo y Previsión Social, buscando unificar de forma sectorial la gestión y el intercambio de información entre ellas. Considerando específicamente la información ofertada y demandada por estas actualmente.
- **Nodo Laboral y Sectorial:** Para unificar la información sectorial que nutre tanto la Ficha Única como otros procesos estatales, se propone implementar un nodo que reciba y comparta la información ofrecida o consumida por las instituciones participantes.
- **Ficha Única:** Como primer caso de uso, la Ficha Única incorporará datos de instituciones clave —como la Superintendencia de Seguridad Social, el IPS, la Dirección del Trabajo y la Superintendencia de Pensiones—, brindando una vista consolidada y estructurada de la información laboral y previsional.

3.2. FUNCIONALIDADES BASE DEL SISTEMA

Apoyándose en los elementos mencionados anteriormente, el sistema de interoperabilidad a diseñar, debe tener las siguientes funcionalidades base:

- **Centralización de la información**

  El sistema debe consolidar los datos de las 11 Organizaciones de la Administración del Estado (OAEs) involucradas en un Datahub único, asegurando el acceso a información estandarizada y actualizada desde un único punto. Esto permitirá que las OAEs accedan a datos completos y consistentes sin recurrir a múltiples fuentes, eliminando duplicidades y optimizando los tiempos de consulta. Por ejemplo, en caso de que una institución registre un cambio en el estado laboral de un ciudadano, esta información podrá ser notificada automáticamente a otras OAEs relevantes agilizando los trámites asociados.

Además, la centralización debe incluir un mecanismo de notificaciones basado en señales, que informe a las instituciones involucradas sobre eventos clave, como actualizaciones de datos o modificaciones en normativas[5] que puedan impactar en sus operaciones. La gobernanza del sistema debe permitir definir reglas claras sobre quién puede acceder a cada señal, garantizando la seguridad y confidencialidad de la información. Por ejemplo, ciertos eventos podrán ser visibles solo para OAEs del sector previsional, mientras que otros podrían estar disponibles para un grupo más amplio de organismos.

- **Visualización de la información en la ficha única:**

  La Ficha Única debe servir como una interfaz centralizada que presente de manera estructurada los datos laborales y previsionales consolidados de las OAEs involucradas. Este diseño permitirá a las instituciones y ciudadanos consultar información clave de forma rápida y comprensible. Por ejemplo, si una persona recibe el Subsidio Único Familiar (SUF), la Ficha Única debe reflejar esta información automáticamente, incluyendo datos relacionados del Ministerio de Desarrollo Social.

  Además, la ficha debe adaptarse a diferentes roles y niveles de acceso, asegurando que cada OAE o ciudadano visualice únicamente los datos pertinentes a su función o derechos. Esto incluye opciones para personalizar la presentación de información según las necesidades de las OAEs, como estadísticas consolidadas para informes internos o vistas simplificadas para atención al público, y la modalidad en que se presenta esto dependiendo si es una institución o un ciudadano. Por ejemplo, las OAE debieran recibir la ficha enviada desde el nodo sectorial a través del sistema PISEE 2.0, no así el ciudadano que lo verá desde una interfaz dedicada.

- **Trazabilidad de la información**

  El sistema debe registrar de forma exhaustiva todas las interacciones con los datos, incluyendo consultas, actualizaciones y transferencias. Cada acción realizada sobre la información debe ser documentada, proporcionando un historial detallado que identifique el origen, el destino, los responsables y el momento en que ocurrió cada cambio. Por ejemplo, si un funcionario accede a los datos de un ciudadano para validar un trámite, esta acción debe quedar registrada junto con su propósito.

  Esto con la finalidad de tener transparencia en el manejo de información y facilitar las auditorías, asegurando el cumplimiento de normativas y políticas de seguridad de la información[6].

[5] Dentro de estas se consideran cambios en normativas que tengan efecto en la estructura, transacción y restricción de acceso a los datos, documentos y expedientes electrónicos.

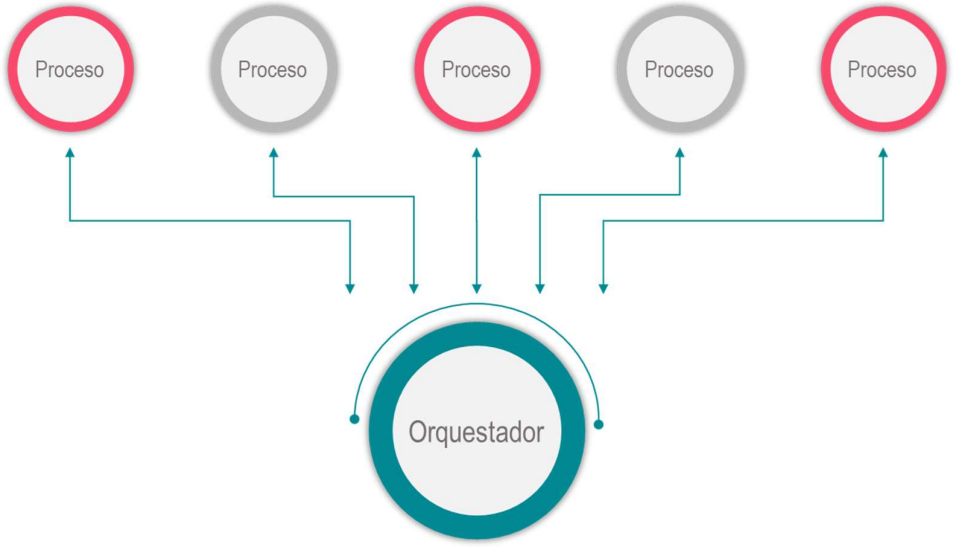
[6] Se entiende por normativas vigentes y políticas de seguridad de la información a las referida a la Ley N°21.180 de Transformación Digital, la Ley N° 21.719 de Protección de Datos Personales, la Política Nacional de Ciberseguridad y, en un futuro, la Ley N° 21.663 que establecerá el Marco de Ciberseguridad, además de la Agencia Nacional de Ciberseguridad.

3.3. Orquestación vs Coreografía de Procesos

Para que estas funcionalidades se implementen con éxito, se deben analizar dos enfoques distintos para coordinar la interacción entre múltiples actores.

- Por un lado, la **orquestación** se basa en un control centralizado ejercido por una entidad que dirige el flujo completo del proceso, asignando tareas y supervisando su ejecución. Este enfoque resulta eficaz cuando los procedimientos están claramente definidos y requieren un control estricto por un ente central para asegurar consistencia y precisión. Sin embargo, su rigidez puede dificultar la adaptación ante cambios imprevistos.

  Por ejemplo, supongamos que el Estado crea un portal único para trámites digitales. Cuando un ciudadano solicita un certificado de antecedentes, un sistema central coordina el proceso: recibe la solicitud, verifica la identidad, consulta a organismos (como la policía y los tribunales) y consolida la información para emitir el certificado. Así, un único "director" supervisa cada paso, facilitando el control del proceso.



  Actualmente, las instituciones del sector laboral y previsional han funcionado bajo este enfoque, procurando avanzar de forma interna con los compromisos de transformación digital, colaborando a través de convenios de intercambio de información con otros organismos.

- Por otro lado, la **coreografía** adopta un modelo descentralizado, en el que cada participante actúa de manera autónoma y coordina sus acciones con el resto a través de lineamientos compartidos. Esta interacción directa, sin un ente central que dicte el orden exacto de las tareas, brinda mayor flexibilidad, autonomía, escalabilidad y capacidad de adaptación a entornos cambiantes. Aún cuando el diseño inicial de una coreografía sea más complejo, a largo plazo ofrece un marco más resiliente,

especialmente útil en sistemas o ecosistemas en constante evolución, donde las organizaciones requieren reaccionar de forma ágil a nuevas condiciones.

Por ejemplo, si el Estado implementara un sistema descentralizado en el que las instituciones actúan de forma coordinada, cuando un ciudadano actualiza sus datos en el Registro Civil, se enviaría una notificación a organismos como el Ministerio de Salud y el Ministerio de Educación. Cada entidad, al recibir la notificación, actualizaría sus registros siguiendo protocolos comunes, permitiendo una sincronización ágil sin necesidad de un coordinador central.

Tomando en cuenta estas características, la propuesta es implementar un **modelo híbrido**. En este escenario, cada institución u organismo mantiene internamente sus propios procesos bajo un modelo de orquestación —con su control, reglas y secuencias internas—, pero al mismo tiempo se integra en un entorno coreográfico más amplio, en conjunto a las demás instituciones del sector.

Esta arquitectura se hace realidad a través de un sistema centralizado (en este caso el nodo laboral y previsional, a través del intercambio de data en PISEE 2.0) que no dicta todos los pasos, sino que proporciona un marco común para que las instituciones intercambien información, se suscriban a eventos y reaccionen a las señales o eventos publicadas por otras. De este modo, el ecosistema global se comporta como una coreografía donde las instituciones comparten información y notifican al resto de las organizaciones a través del nodo sectorial flexibilizando el intercambio de datos, documentos y expedientes, mientras que cada institución orquesta sus actividades internas, utilizando lo que resulte relevante para sus funciones.

Este enfoque híbrido aprovecha las fortalezas de ambos modelos:

- Desde la perspectiva individual, cada organismo conserva el control sobre sus procesos, garantizando orden interno y cumplimiento de sus propios estándares.
- Desde la perspectiva sistémica, se logra una interacción fluida entre las instituciones, que pueden adaptarse con mayor facilidad a cambios en el entorno, compartir información sin generar nuevos cuellos de botella y colaborar de forma dinámica bajo lineamientos generales compartidos.

3.4. Sistema de Eventos y Señales

Para que la coreografía de procesos entre instituciones funcione sin depender de un ente central, se propone un sistema interinstitucional de Publicación/Suscripción (Pub/Sub) que facilite la comunicación y coordinación. Esta solución responde a las limitaciones actuales en la tramitación de procedimientos compartidos entre varias instituciones, donde la falta de flujos automatizados de información genera ineficiencias y afecta la experiencia ciudadana.

El sistema se basa en un “mercado de señales” centralizado, a través del cual las instituciones emiten y reciben notificaciones sobre el estado de sus procesos administrativos de forma estandarizada. De esta manera, se eliminan acuerdos bilaterales individuales, reduciendo la complejidad burocrática y fomentando la innovación.

Gracias al modelo Pub/Sub, las instituciones publican señales al completar trámites o alcanzar hitos, mientras que otras, al suscribirse, pueden reaccionar automáticamente a estos eventos. Así se establece una coreografía que optimiza la coordinación interinstitucional, manteniendo la autonomía interna de cada organismo.

La gobernanza del sistema determina el acceso a las señales según las competencias de cada institución, garantizando la seguridad y el cumplimiento normativo. Asimismo, la trazabilidad integral posibilita auditar y monitorear las comunicaciones.

Este enfoque aporta beneficios tanto a las instituciones—simplificando la gestión y mejorando la eficiencia—como a la ciudadanía, al agilizar trámites y eliminar redundancias innecesarias. A la vez, la integración con el hub de datos central y la compatibilidad con sistemas existentes posibilitan una adopción gradual, comenzando con instituciones piloto y extendiéndose de manera controlada. De esta forma, el sistema de señales se concibe como un componente opcional para aquellas entidades que estén listas para implementarlo, mientras que el resto puede seguir consumiendo los servicios a través de PISEE. Para apoyar la adopción de esta solución, la plataforma incluirá piezas de código que faciliten la conexión con el nodo laboral, junto con cápsulas informativas que orienten sobre cómo llevar a cabo dicha integración.

4. ARQUITECTURA DEL SISTEMA INTEROPERABLE PROPUESTO

La siguiente sección describe las propuestas de arquitectura técnica y las interacciones entre componentes, mostrando cómo la infraestructura conversa para cumplir con las funcionalidades bases del sistema, reflejo de los bosquejos propuestos en conjunto con el equipo de SPS.

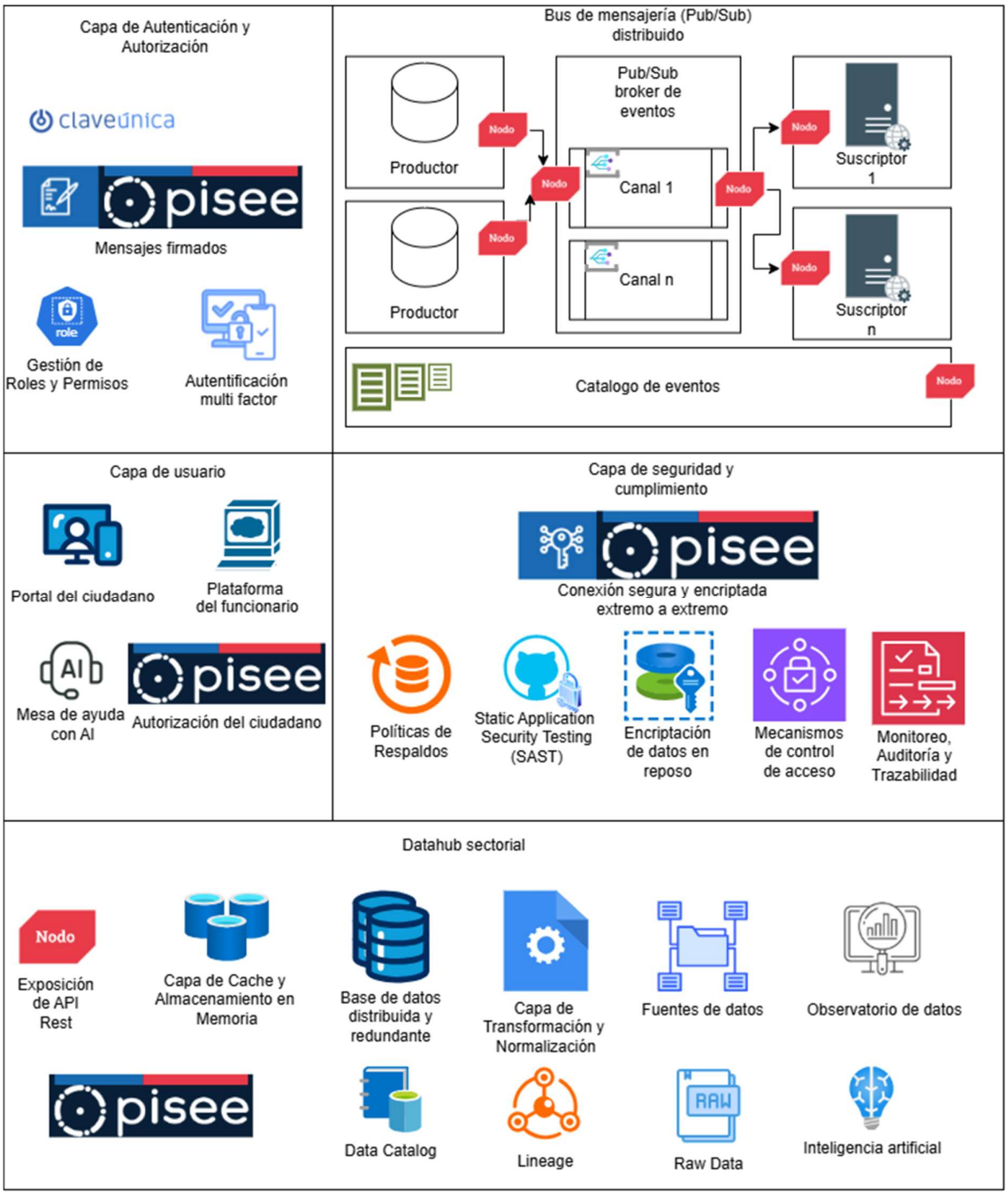
Esta tiene por objetivo diseñar un ecosistema tecnológico que facilite el intercambio seguro, oportuno y estandarizado de información entre las diversas instituciones del sector laboral y previsional, consolidando dichos datos en una “Ficha Única”. Esta ficha será accesible de manera centralizada a través de la plataforma PISEE 2.0, respetando estándares abiertos y siguiendo un modelo que soporte tanto la orquestación como la transición hacia un modelo más coreográfico de interoperabilidad.

4.1. PRIMERA PROPUESTA DE ARQUITECTURA

La primera propuesta de arquitectura se basa en un ecosistema distribuido, soportado por un bus de mensajería (Pub/Sub) que posibilita la coreografía de procesos entre instituciones. Esto permite un intercambio de datos fluido, sin requerir acuerdos bilaterales específicos, ya que las instituciones pueden publicar eventos y suscribirse a señales de interés. Adicionalmente, incluye un nodo sectorialque consolida información sectorial en una Ficha Única, capaz de seguridad integradas con PISEE 2.0 para garantizar confidencialidad y trazabilidad, transformación de datos, un catálogo central, linaje, y capacidades de observación y análisis.

Esta arquitectura refuerza la gestión responsable de los datos mediante la trazabilidad y medidas de seguridad avanzadas integradas desde el diseño. Al consolidar información sectorial en una Ficha Única y garantizar un intercambio eficiente mediante un bus de mensajería, se elimina la redundancia en los procesos administrativos, cumpliendo con los principios de interoperabilidad y eficiencia establecidos en la normativa actual[7]. Este enfoque asegura que las operaciones sean ágiles y precisas, respetando los fines específicos de tratamiento y fortaleciendo la coordinación interinstitucional bajo un marco legal sólido.

[7] Ley 21.719, Artículos 21 y 14 quinquies: Principios de interoperabilidad, seguridad y eficiencia.



4.1.1. Principios Base de la propuesta

1. **Desacoplamiento mediante mensajería orientada a señales o eventos (Pub/Sub)**: La arquitectura se basa en un bus de mensajería distribuido que permite a las instituciones publicar eventos y señales sin necesidad de conocer los consumidores finales. Las demás instituciones y el Datahub se suscriben a estos canales y reaccionan cuando los datos o estados cambian, habilitando un modelo coreográfico en vez de uno fuertemente orquestado.
2. **Alta disponibilidad y resiliencia**: Se diseña la infraestructura para tolerar fallas, garantizando continuidad en la

operación del nodo sectorial y el intercambio de información. Bases de datos distribuidas, nodos redundantes, replicación de datos y mensajería confiable aseguran que el sistema siga funcionando incluso ante caídas parciales de componentes.

3. **Integración con PISEE para seguridad y trazabilidad**: El ecosistema se conecta a través de la Plataforma de Intercambio Seguro del Estado (PISEE), que ofrece cifrado extremo a extremo, autenticación y autorización centralizada. Esto permite un intercambio de información confiable, con mensajes firmados y trazabilidad de interacciones entre instituciones, asegurando el cumplimiento normativo.
4. **Enfoque en la Ficha Única y la interoperabilidad**: La arquitectura se centra en consolidar información desde múltiples instituciones en una Ficha Única, ofrecida a través de APIs expuestas por el Datahub. El uso de estándares abiertos y políticas de interoperabilidad posibilita que distintas entidades del sector trabajo se integren sin necesidad de acuerdos bilaterales complejos.
5. **Capacidad de manejar datos en tiempo real y datos históricos**: Además del flujo transaccional, la arquitectura incluye un catálogo de datos, linaje, capa de transformación y normalización. Esto permite no sólo servir datos operativos en tiempo real (con caché y validación de vigencias) sino también gestionar información histórica, cargas masivas y análisis avanzado para ciertas fuentes de información que puedan ser almacenadas.

4.1.2. Capa de Autenticación y Autorización

La capa de Autenticación y Autorización se refuerza incorporando autenticación multifactor y mensajes firmados electrónicamente por PISEE 2.0 para el intercambio seguro de información entre instituciones. Para el acceso por parte de personas naturales (ciudadanos), se mantendrá el uso de Clave Única para accesos web, garantizando un control de identidades centralizado, mientras que para los funcionarios públicos se agrega un segundo factor de autenticación, por ejemplo, a través correo electrónico institucional, fortaleciendo así el nivel de seguridad y permitiendo validar que el funcionario siga siendo empleado de la OAE. Además, se gestionarán perfiles y permisos granulares basados en roles (RBAC), lo que permitirá delimitar acciones específicas según las funciones del usuario dentro de la organización, asegurando el principio de mínimo privilegio. Los roles propuestos son:

1) **Administrador Sectorial**: Rol de más alto nivel dentro del sector del trabajo. Puede asignar o revocar roles a las instituciones participantes, aprobar la incorporación de nuevos servicios, gestionar el catálogo de datos y definir políticas globales de seguridad, trazabilidad y cumplimiento normativo.
2) **Coordinador de Transformación Digital (Institución)**: Encargado de administrar los usuarios y recursos al interior de una institución específica. Puede asignar roles a funcionarios internos, supervisar el acceso a los datos de su institución, suscribirse o darse de baja de ciertos flujos de señales, y asegurar el cumplimiento de las políticas establecidas.
3) **Funcionario Público Operativo**: Accede a la información necesaria para la tramitación de procedimientos específicos. Puede consultar la información del Nodo Sectorial relacionada con su ámbito de trabajo, actualizar estados de trámites, agregar documentación asociada y emitir señales relativas al avance de procedimientos. No

puede acceder a información que exceda su ámbito de competencia ni modificar datos ajenos a su función.

4) **Analista de Datos**: Permiso para consultar información curada y consolidada en el datahub con fines analíticos. Puede generar reportes, métricas e indicadores, sin capacidad para modificar datos de operación o realizar cambios en la configuración del sistema.
5) **Auditor / Control Interno**: Acceso de sólo lectura a registros históricos, logs de auditoría, trazabilidad de mensajes y documentos, con el propósito de verificar el cumplimiento normativo y la integridad de los procesos. Carece de permisos para alterar datos o ajustar configuraciones.
6) **Ciudadano**: Permisos limitados para consultar únicamente su información personal (Ficha Única), revisar el estado de sus trámites y eventualmente actualizar ciertos datos personales de contacto. No tiene acceso a información de terceros ni a datos internos de las instituciones.

Por otro lado, la autorización del intercambio de información entre instituciones se implementará mediante el uso de mensajes firmados electrónicamente por PISEE. Estos mensajes, encriptados y con firma digital, garantizarán la integridad, autenticidad y no repudio de la información compartida. Asimismo, la compatibilidad con los servidores de autorización y certificados administrados por PISEE permitirá que las instituciones cumplan con las políticas de seguridad y trazabilidad, establecidas a nivel nacional, fortaleciendo la interoperabilidad y la confianza en el ecosistema digital del Estado.

4.1.3. Bus de Mensajería (Pub/Sub) Distribuido

La capa del bus de mensajería Pub/Sub distribuido genera la capacidad de coreografía de procedimientos administrativos entre las instituciones y el Datahub. Esta capa está diseñada para operar con alta disponibilidad y resiliencia, soportando un esquema de publicación-suscripción que permite que cualquier OAE emita eventos a un catálogo de canales predefinidos. Cada evento está debidamente documentado en el catálogo, con información sobre su semántica, formato de datos, origen, tipos de consumidores potenciales, y políticas de retención. De esta forma, las instituciones pueden suscribirse a los canales relevantes, recibiendo notificaciones en tiempo real que les permitan reaccionar de manera automatizada ante cambios en el ecosistema de datos, sin tener que establecer convenios bilaterales o estar consultando constantemente por cambios de estados. Esta arquitectura facilita el modelo coreográfico entre instituciones, ya que cada una responde a los eventos según sus propias reglas de negocio, manteniendo su autonomía. Esto también permite que cada OAE diseñe nuevos servicios de cara al ciudadano sin necesidad de coordinación previa en base a las señales y eventos que estén disponibles.

En este escenario, el nodo sectorial actúa también como un emisor clave, publicando eventos que informan, por ejemplo, sobre la actualización de una fuente de datos sectorial, cambios en la Ficha Única o la disponibilidad de nuevas fuentes de información. Entre los canales que podrían existir, se incluyen:

- **Canal "Actualización Laboral"**: Empleado por instituciones como la Dirección del Trabajo (DT), la Superintendencia de Pensiones (SP) y el Instituto de Previsión Social

(IPS) para notificar cambios en el estado laboral de un contribuyente, finalización de procedimientos administrativos o emisión de nuevos certificados.

- **Canal "Cambios Previsionales"**: Utilizado para eventos que reflejan variaciones en la información previsional de los ciudadanos, como el registro de cotizaciones, procesos de recálculo de pensiones, la disponibilidad de nuevos datos del seguro de cesantía (AFC) y de acceso a otros beneficios laborales y/o previsionales.
- **Canal "Alertas y Seguimiento de Trámites"**: Cuando un trámite pasa una etapa clave, se publica un evento para que las instituciones responsables del siguiente paso se activen. Por ejemplo, si la DT concluye la verificación de un contrato laboral, se emite una señal para que el IPS inicie el cálculo de cotizaciones o la AFC actualice la situación previsional del trabajador.
- **Canal "Novedades Datahub"**: Emitido por el Datahub mismo, para informar que se han actualizado fuentes de datos, permitiendo que otras instituciones y sistemas de análisis reaccionen, por ejemplo, ajustando sus flujos ETL o alertando a funcionarios sobre información recién consolidada.

Algunos de caso de uso concreto son los siguientes:

1. **Procedimiento Administrativo Detenido por Falta de Información**
    a. **Canal:** `procedimientos_laborales`
    b. **Evento Emitido:** `certificacion_previsional_actualizada`
    c. **Descripción:**
    La Dirección del Trabajo (DT) ha iniciado un procedimiento administrativo para un ciudadano y requiere la certificación previsional de la Superintendencia de Pensiones (SP). Sin las señales, el ciudadano tendría que solicitar el documento en la SP y luego llevarlo físicamente a la DT. Con el sistema Pub/Sub, la DT se suscribe al canal `procedimientos_laborales` para recibir el evento `certificacion_previsional_actualizada` asociado a ese ciudadano. Una vez que la SP actualiza la información previsional en el Datahub, éste emite el evento en dicho canal, la DT lo recibe de inmediato y puede continuar el trámite sin que el ciudadano intervenga nuevamente.
2. **Actualización Masiva de Datos y Notificación al Ecosistema**
    a. **Canal:** `datahub_novedades`
    b. **Evento Emitido:** `fuente_ips_actualizado`
    c. **Descripción:**
    El Instituto de Previsión Social (IPS) realiza una actualización masiva de sus bases, incorporando nuevos registros sobre pensiones y cotizaciones. Tras finalizar el proceso, el Datahub emite la señal `fuente_ips_actualizada` en el canal `datahub_novedades`. Instituciones como el IPS o la DT, suscritas a este canal, reciben la notificación y pueden reaccionar automáticamente: refrescar sus cachés, recalcular indicadores o ajustar sus procesos internos. De este modo, la información está disponible y reconocida por el ecosistema sin pasos manuales adicionales.
3. **Notificación sobre la Fecha Próxima de Pago de un Subsidio**
    a. **Canal:** `subsidios_eventos`
    b. **Evento Emitido:** `fecha_pago_subsidio_modificado`

c. **Descripción:**
el IPS actualiza la fecha de pago de un subsidio importante. Al confirmarse esta modificación, el Datahub emite el evento `fecha_pago_subsidio_modificada` en el canal `subsidios_eventos`. Instituciones como la SUSESO o Chile Atiende, que necesitan conocer esta fecha para comunicar a los beneficiarios, se enteran al instante. Esto permite ajustes automáticos en cronogramas internos, envío de notificaciones a ciudadanos, o actualizaciones en portales informativos, sin requerir comunicación directa entre instituciones.

Con esta arquitectura, las instituciones no dependen de flujos rígidos ni de peticiones sincronizadas entre sí (sincronizadas por la visita de un ciudadano), sino que pueden reaccionar dinámicamente a la llegada de eventos relevantes. Esto acelera el intercambio de información, reduce la burocracia y facilita la gestión proactiva de procesos en el ecosistema Laboral y Previsional.

4.1.4. Capa de Usuario

La capa de usuarios abarca todos los puntos de interacción directa entre personas (ciudadanos, funcionarios) o servicios de apoyo y el ecosistema del Nodo Sectorial, garantizando una experiencia consistente, segura y accesible. En primer lugar, el **Portal del Ciudadano** brinda a las personas un acceso centralizado a sus datos laborales y previsionales a través de la Ficha Única disponibilizada en un formato web y mobile. Aquí, el ciudadano puede consultar el estado de sus trámites, revisar documentación asociada y recibir notificaciones en la aplicación móvil de eventos relevantes (por ejemplo, fechas de pagos de subsidios, nuevos subsidios pendientes, etc), todo autenticándose con Clave Única.

En casos específicos, donde se requiera compartir datos personales con una institución, se propone una autorización explícita por parte del ciudadano usando los siguientes medios:

- **Clave Única:** al momento de realizar un trámite electrónico con una institución que requiera la clave, donde el ciudadano pida información a esta, se solicitará el consentimiento explícito del uso de información.
- **Presencialmente en la OAE:** Cuando se deba realizar el trámite presencial y se requiera información de la persona proveniente de otras OAEs, se solicitará el consentimiento a este para obtener la información usando su Clave Única.
- **Por medio de PISEE 2.0:** Infraestructura en desarrollo por el Gobierno Digital, que ofrecerá un sistema seguro y transparente para que el ciudadano controle quién accede a su información,El ciudadano también puede actualizar información personal relevante como información de contacto o desuscripción a qué información sea compartida con otras instituciones, en línea con los derechos de acceso y oposición establecidos en la ley de protección de datos[8]

Es importante destacar que, al ingresar con Clave Única (electrónica y presencialmente), la entidad recibe un token que envía en la solicitud de información al Nodo Sectorial, el cual aprueba el acceso a la Ficha Única.

Por su parte, la **Plataforma del Funcionario** es una interfaz dedicada al personal de las instituciones del sector trabajo. A través de esta, los funcionarios, autenticados con Clave Única y factor adicional de seguridad (MFA), acceden a herramientas internas, tableros de control, expedientes electrónicos y administración de fuentes de información.

Además, la **Mesa de Ayuda con AI** proporciona asistencia automatizada para consultas frecuentes, guiando a ciudadanos y funcionarios en el uso de la plataforma, la resolución de problemas y la optimización de procesos. Este front-end asistido por inteligencia artificial, integrado con la capa de datos y el registro de eventos, ayuda a resolver dudas, escalar casos complejos a soporte humano y, en general, mejorar la experiencia de usuario. Con estas soluciones en conjunto, la capa de usuarios garantiza usabilidad, seguridad, control de la información y eficiencia en la entrega de servicios digitales del Estado. Esta mesa de ayuda puede ser administrada por alguna institución del ecosistema como lo es Chile atiende.

4.1.5. Capa de Seguridad y Cumplimiento

La capa de seguridad y cumplimiento constituye el núcleo que garantiza la protección integral de los datos, la resiliencia operativa y el cumplimiento normativo dentro del ecosistema del Datahub. Este módulo integra políticas, tecnologías y procedimientos diseñados para salvaguardar la confidencialidad, integridad y disponibilidad de la información, al mismo tiempo que asegura la adhesión a marcos legales y estándares técnicos establecidos por el Estado.

- **Conexión segura y encriptada extremo a extremo (PISEE)**: El canal principal de comunicaciones entre el Datahub, las instituciones y los usuarios

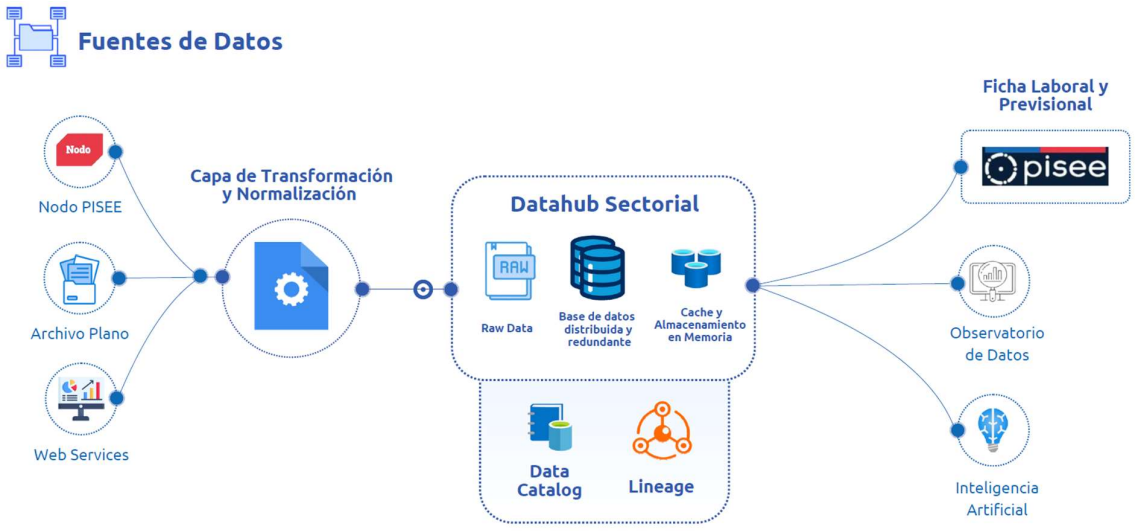
[8] Ley 21.719, Artículos 4° y 5°: Derechos del titular de datos personales.

finales se encuentra protegido por PISEE (Plataforma de Intercambio Seguro del Estado), que garantiza la confidencialidad y la autenticidad de las interacciones mediante criptografía de alto nivel. Esto evita accesos no autorizados, intercepciones maliciosas y proporciona un medio confiable de intercambio de datos, documentos y señales interinstitucionales.

- **Políticas de Respaldos**: Se establecen procedimientos de respaldos periódicos, almacenamiento redundante y planes de recuperación ante desastres que permiten restaurar rápidamente la operación en caso de fallos técnicos, ciberataques o eventos fortuitos. Esta estrategia asegura la disponibilidad constante de la información y minimiza el impacto ante incidentes.
- **Static Application Security Testing (SAST)**: Antes de la puesta en producción de servicios y aplicaciones, se aplican análisis de seguridad estáticos al código (SAST) para detectar vulnerabilidades, fallos lógicos o configuraciones inseguras. Esto permite corregir problemas temprano en el ciclo de desarrollo, reduciendo riesgos y garantizando un software robusto.
- **Encriptación de Datos en Reposo**: Todos los datos almacenados en el Datahub, ya sean registros transaccionales, documentos o métricas analíticas, se cifran en reposo. Esto dificulta el acceso a la información por parte de actores no autorizados incluso si se obtuviera acceso físico a los dispositivos de almacenamiento.
- **Mecanismos de Control de Acceso**: Se implementan sistemas centralizados de autenticación, autorización y gestión de identidades, incluyendo autenticación multifactor y asignación de roles y permisos basados en el principio de mínimo privilegio. Además, la trazabilidad de acciones y el registro de eventos de seguridad respaldan la detección temprana de comportamientos anómalos.
- **Monitoreo, Auditoría y Trazabilidad**: Se monitorizan continuamente las operaciones del Datahub, recolectando logs, métricas y eventos para su análisis. Herramientas de auditoría y trazabilidad permiten inspeccionar el historial de accesos, uso de datos y ocurrencias de ciberseguridad, facilitando la detección de incidentes, investigaciones forenses y el aseguramiento del cumplimiento normativo.

4.1.6. Nodo Sectorial

El Nodo sectorial se compone de múltiples módulos que colaboran para integrar, almacenar, transformar, exponer y analizar la información laboral y previsional. Estos componentes están diseñados para garantizar disponibilidad, calidad, trazabilidad y eficiencia en el acceso a datos consolidados.



1. **Exposición de API Rest con la ficha por PISEE 2.0**: A través de este módulo, el Datahub expone una interfaz unificada (APIs RESTful) para ofrecer la Ficha Única del ciudadano. La interacción se realiza mediante PISEE, garantizando seguridad, autenticación y cifrado de extremo a extremo. Esto asegura que las instituciones y ciudadanos accedan a información consistente y actualizada, manteniendo la confidencialidad y la integridad de los datos.

2. **Capa de Caché y Almacenamiento en Memoria**: Para acelerar las respuestas a las consultas más frecuentes, esta capa almacena datos clave en memoria (ej. Redis, Hazelcast). Así se reducen tiempos de respuesta y se evita acceder repetidamente a las fuentes originales. Los datos cacheados tienen una vigencia configurada, respetando políticas de expiración para asegurar que la información mantenida en memoria siga siendo confiable.

3. **Data Catalog**: Un catálogo centralizado que describe las fuentes de datos, su contenido, esquemas, transformaciones y políticas de acceso. Permite a las instituciones descubrir y entender qué información está disponible, su nivel de calidad y cómo puede ser consumida, facilitando la gobernanza y asegurando el cumplimiento normativo.

4. **Lineage (Linaje de Datos)**: Este componente registra el recorrido completo de la información: desde su origen (fuente bruta), pasando por las distintas capas de transformación, hasta llegar a la Ficha Única. De esta manera, se pueden trazar los pasos que sufrió el dato, detectar inconsistencias, comprender su contexto y facilitar auditorías y verificaciones.

5. **Raw Data**: La capa de datos en bruto (raw data) almacena la información tal cual se recibe de las fuentes, sin modificaciones. Esto permite reprocesar o aplicar nuevas transformaciones si cambian las reglas de negocio, así como auditar la información

original en caso de discrepancias o mejoras futuras. Se debe definir una política, para cada fuente de datos, del tiempo de almacenamiento del dato.

6. **Base de Datos Distribuida y Redundante**:
   Una base de datos escalable y con replicación entre nodos garantiza la alta disponibilidad y la tolerancia a fallos. La información se almacena de manera consistente, evitando puntos únicos de falla y asegurando que, ante una contingencia, los datos sigan siendo accesibles y confiables.

7. **Capa de Transformación y Normalización**:
   En esta capa se limpian, validan, estandarizan y enriquecen los datos provenientes de múltiples fuentes. Mediante procesos ETL (Extract Transform Load), se generan conjuntos de datos coherentes, alineados con los modelos semánticos sectoriales, listos para su consumo a través de la Ficha Única.

   La estrategia para este Datahub será modificar lo menos posible la fuente de información de origen, es decir, no se modificará el contenido del mensaje, solo se filtrarán columnas y se tratará de escoger las columnas de cada fuente de información que dicha OAE sea la responsable de entregar. Por ejemplo, la mayoría de las fuentes de información dirán un nombre y sexo, donde puede haber inconsistencia entre las distintas fuentes de información de las otras OAEs, pero si se cuenta con la fuente de información original (en este caso Registro Civil) se considerará esta como el dato origen y se descartarán las columnas “nombre” y “sexo” de las otras fuentes de información.

8. **Fuentes de Datos**:
   Las fuentes de datos que alimentan el Datahub pueden presentar distintas características en cuanto a su origen, naturaleza de la información y frecuencia de actualización. Estas diferencias influyen en la estrategia de integración, el modelo de procesamiento y el uso eficiente de las capacidades de almacenamiento y caché.
   a. **Tipos de Datos:**
      i. **Datos Transaccionales (On-Demand):**
         Estos datos se obtienen en tiempo real o bajo demanda en el momento exacto en que se consulta la Ficha Única o se requiere procesar un evento. Por ejemplo, cuando un ciudadano solicita el estado actual de su trámite laboral, el Datahub consulta directamente la fuente de información más reciente. Este enfoque es ideal para datos que cambian con frecuencia o información que depende de condiciones dinámicas, como la situación previsional actualizada al minuto o un trámite administrativo que puede modificarse entre una consulta y otra. La recomendación es configurar una capa de caché con una vigencia corta, de modo que las consultas reiteradas durante un intervalo de tiempo limitado no saturen las fuentes originales, pero asegurando que los datos se invaliden con rapidez para reflejar cualquier cambio reciente.
      ii. **Cargas Masivas (Batch):**
         Estas se aplican a datos que no cambian con frecuencia o cuyo ciclo de vida es más estable. Por ejemplo, la información histórica de subsidios otorgados o de afiliaciones previsionales consolidadas. En

estos casos, se pueden realizar cargas completas o incrementales con una periodicidad definida (diaria, semanal, mensual). Una vez incorporados al Datahub, estos datos pueden almacenarse en la capa de datos en bruto y en versiones procesadas, para luego ser cacheados y consultados sin necesidad de acudir continuamente a la fuente original.

Por ejemplo, si un subsidio está asignado a una persona y su condición es estática (no se "desasigna" una vez otorgado), se puede consolidar esta información a través de una carga masiva nocturna. De esta manera, las futuras consultas a la Ficha Única obtendrán el dato rápidamente desde la memoria caché o desde el Datahub, sin necesidad de re-consultar la fuente transaccional. Si un ciudadano no tiene subsidios asignados, en vez de mantener esa ausencia de información en memoria, el Datahub puede optar por una consulta transaccional on-demand la primera vez que se solicita esa información y cachear el resultado (por ejemplo, "ningún subsidio asignado") por un periodo breve.

Este tipo de fuente solo es permitida si es que la fuente de información de la OAE puede ser almacenada.

b. **Tipos de Fuentes:**
   i. **Web Services (APIs REST/SOAP):** Muchas instituciones exponen sus datos mediante servicios web. Estos son ideales para datos transaccionales o para consultas específicas al momento de requerir información. Suelen contar con mecanismos de autenticación y autorizaciones que garantizan el acceso seguro. Las interacciones con servicios web son fáciles de rastrear, monitorear y actualizar a medida que cambian las definiciones de la API.
   ii. **Nodo de PISEE 2.0:** El Nodo PISEE 2.0 actúa como intermediario seguro entre las instituciones, proporcionando una capa unificada para la obtención de datos. Aquí pueden publicarse y consumirse servicios, documentos y notificaciones, asegurando la interoperabilidad. La conexión a través de PISEE garantiza trazabilidad, encriptación y autenticación robusta, reduciendo la necesidad de conexiones punto a punto individuales.
   iii. **FTP / SFTP / Secure Fileshare:** Algunas instituciones pueden entregar grandes volúmenes de información mediante cargas masivas en archivos planos (CSV, JSON, XML, Parquet) depositados en servidores FTP/SFTP o repositorios compartidos seguros. Este mecanismo suele emplearse para datos que se actualizan con poca frecuencia o son de carácter histórico. El Datahub puede consumir estos archivos periódicamente, procesarlos e incorporarlos en su repositorio interno.
c. **Recomendaciones del manejo de fuentes de información:**
   i. Para datos estáticos o con poca frecuencia de cambio (ej. subsidios asignados, afiliaciones estables), priorizar la carga masiva y

almacenamiento en caché. Así se evita consultar continuamente la fuente original y se mejora el tiempo de respuesta.

ii. Para datos dinámicos (estado de trámites, información que cambia con la situación laboral diaria), realizar consultas transaccionales y mantener una caché de corta vigencia.

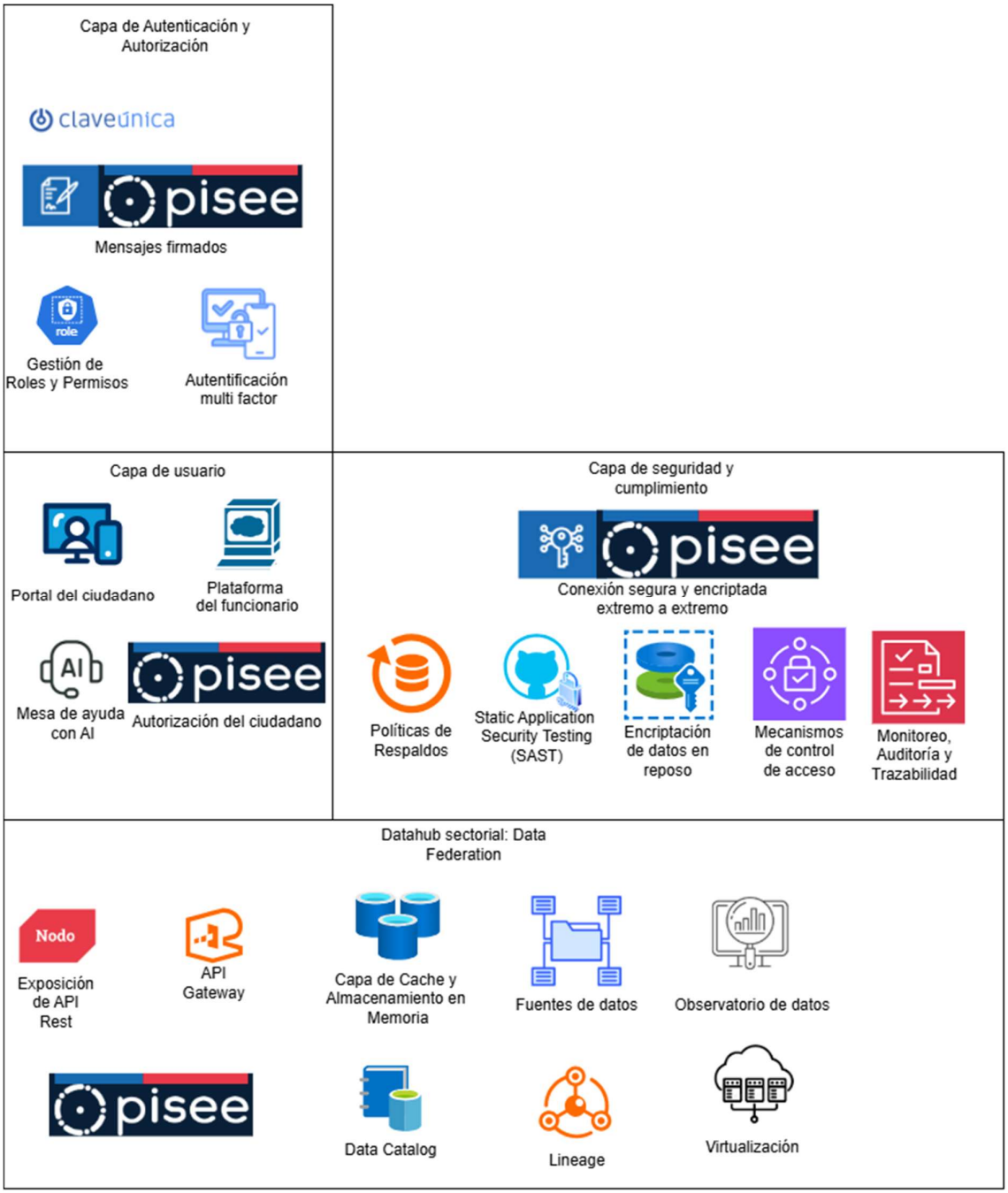
iii. Definir políticas de vigencia y caducidad para cada fuente de datos, tanto transaccional como masiva. Un dato cacheado debería tener un tiempo de vida acorde a su frecuencia de actualización y a las necesidades de precisión del negocio. Por ejemplo, un subsidio asignado podría ser cacheado durante semanas sin necesidad de volver a confirmarlo, mientras que una cotización previsional podría requerir renovarse diariamente.

iv. Escalar el consumo de datos a través de PISEE 2.0 para asegurar una capa de seguridad, trazabilidad y estandarización, reduciendo la complejidad de mantener múltiples integraciones directas.

v. Monitorear y auditar el uso de datos masivos para ajustar la periodicidad de las cargas, el tamaño de las particiones y el nivel de detalle conservado, alineándose con las necesidades analíticas y operativas del DataHub.

4.2. Segunda propuesta de Arquitectura

La segunda propuesta se centra en una federación de APIs y virtualización de datos, minimizando el uso de mensajería. En esta arquitectura, el Datahub actúa como un punto unificado de acceso y consulta, utilizando un API Gateway y una capa de virtualización para integrar las distintas fuentes, ya sean consultadas transaccionalmente o a través de cargas masivas. De esta forma, se reduce la dependencia de eventos y señales, y se opta por un modelo basado en la obtención on-demand y el cacheo inteligente de información estable. La seguridad y la autenticación, incluidas MFA y autorización por PISEE, se mantienen, mientras que el énfasis recae en simplificar la operación y favorecer un acceso centralizado y directo, sin coreografías entre instituciones.


Capa de Autenticación y Autorización
claveúnica
pisee
Mensajes firmados
role
Gestión de Roles y Permisos
Autentificación multi factor
Capa de usuario
Portal del ciudadano
Plataforma del funcionario
AI
Mesa de ayuda con AI
pisee
Autorización del ciudadano
Capa de seguridad y cumplimiento
pisee
Conexión segura y encriptada extremo a extremo
Políticas de Respaldos
Static Application Security Testing (SAST)
Encriptación de datos en reposo
Mecanismos de control de acceso
Monitoreo, Auditoría y Trazabilidad
Datahub sectorial: Data Federation
Nodo
Exposición de API Rest
API Gateway
Capa de Cache y Almacenamiento en Memoria
Fuentes de datos
Observatorio de datos
pisee
Data Catalog
Lineage
Virtualización

4.2.1. Principios Base de la segunda propuesta

- **Federación de Datos y APIs**: En lugar de un bus de mensajería distribuido y una fuerte capa de coreografía basada en señales, la segunda arquitectura prioriza el acceso unificado a los datos mediante un catálogo central y la virtualización de datos. Las fuentes permanecen en sus repositorios originales y el Datahub actúa más como un "punto de integración" que concentra el acceso, exponiendo APIs estandarizadas.
- **Reducción de Dependencia en Mensajería**: Se minimiza el uso de eventos Pub/Sub. En su lugar, las interacciones son mayormente síncronas, basadas en APIs. Para notificaciones críticas, se podrían mantener canales simples de notificación a través de PISEE, pero sin un ecosistema complejo de tópicos y colas.
- **Data Virtualization y Caching**: Se implementa una capa de virtualización de datos que permite acceder a múltiples fuentes (web services, bases de datos, cargas FTP/SFTP) como si fueran una única vista lógica. Esta capa puede aplicar lógicas de caché inteligente para datos poco cambiantes (ej. subsidios asignados) sin requerir una ingesta masiva previa.
- **Herramientas ETL Simplificadas**: Para datos realmente estables (ej. catálogos maestros, información histórica de subsidios no modificables), se ejecutan procesos ETL periódicos para cargarlos en un repositorio central caché (posiblemente una base de datos optimizada para lectura). Estos procesos son más simples y no requieren un ecosistema complejo de streaming, ya que la mayor parte de la consulta se hace bajo demanda.

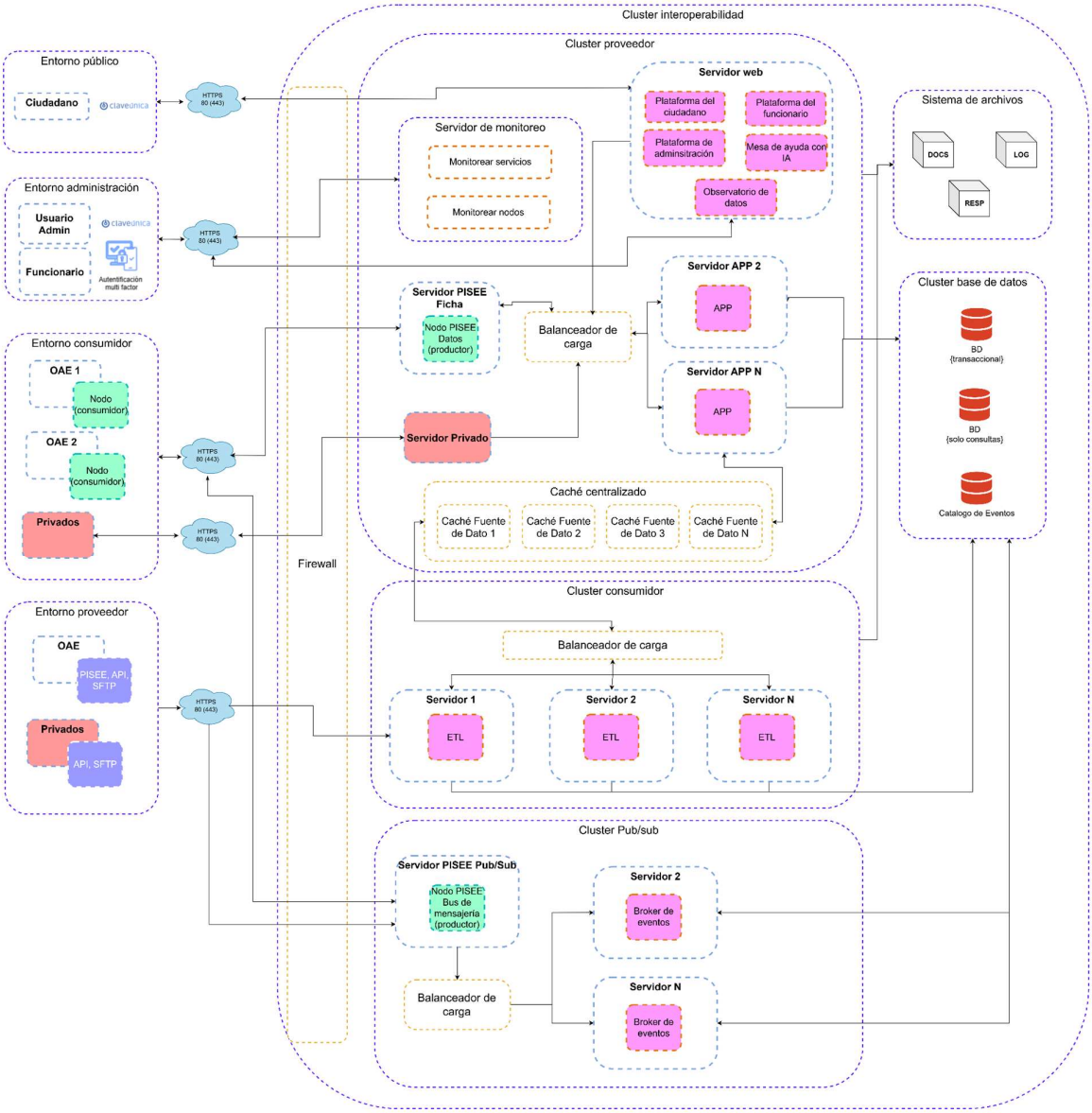
4.2.2. API Gateway y Federador de APIs

Un API Gateway central controla el acceso a las distintas fuentes. Internamente, un federador de APIs (Data Federation Layer) se conecta a las diferentes instituciones (vía PISEE, WS internos, etc.) y construye vistas lógicas. El ciudadano, el funcionario o el sistema consulta la Ficha Única contra estas vistas federadas, y el sistema resuelve las peticiones llamando en tiempo real a las fuentes de datos necesarias.

4.2.3. Capa de Virtualización

Una plataforma de virtualización permite tratar múltiples orígenes como uno solo. Así, la Ficha Única puede construirse sin mantener una copia completa de los datos: la capa de virtualización consulta las fuentes requeridas. Para datos estables (ej. subsidios otorgados) se mantienen copias cacheadas con una vida útil mayor. Para datos dinámicos (ej. estado de un trámite), se consulta on-demand.

5. INFRAESTRUCTURA Y TECNOLOGÍA



5.1. Estructura general

El diagrama define una infraestructura distribuida para la interoperabilidad entre las OAE. Esta infraestructura tiene cuatro entornos principales:

- **Cluster interoperabilidad**: Se encarga de gestionar y facilitar el intercambio seguro y eficiente de datos entre los nodos pertenecientes a diferentes Órganos de la Administración del Estado (OAE).
- **Entorno Consumidor**: Donde los nodos consumen los datos que provienen de otros OAEs.
- **Entorno Proveedor**: Donde los OAEs exponen datos mediante servicios como PISEE, API o SFTP.

- **Entorno Administración:** Corresponde a los usuarios que administren la plataforma, ya sean funcionarios de alguna OAE que configuran sus fuentes de información o bien usuarios administradores que monitorean o dan privilegios a otros usuarios en la plataforma. El acceso por este medio es con autenticación multi factor.

- **Entorno Público:** Corresponde a los accesos de los ambiente web de la plataforma por parte de los ciudadanos. Este es el acceso donde cada usuario puede ver su propia información. El acceso por este medio es con clave única.

Estos entornos están conectados mediante un **Cluster de Interoperabilidad**, que sirve como intermediario entre consumidores y proveedores.

5.1.1. Descripción del Cluster de Interoperabilidad

El **Cluster de Interoperabilidad** es el núcleo de la infraestructura que facilita el intercambio de datos entre los Órganos de la Administración del Estado (OAE). Corresponde a la intranet de la solución. Está diseñado para garantizar la conectividad, seguridad, procesamiento eficiente y escalabilidad en las operaciones de consumo y provisión de datos. Este cluster incluye múltiples componentes que trabajan en conjunto para cumplir con los requerimientos funcionales y no funcionales de interoperabilidad.

5.2. Componentes del Cluster de Interoperabilidad

El cluster se divide en dos subcomponentes principales: el **Cluster Proveedor** y el **Cluster Consumidor**, además de otros servicios auxiliares.

5.2.1. Cluster Proveedor

Este subcomponente es responsable de procesar, almacenar y exponer los datos provenientes de los OAEs proveedores de información.

- **Servidor PISEE Ficha:** Corresponde al servidor que disponibiliza el endpoint de la ficha en PISEE. Este tiene escalamiento vertical y cumple la función de middleware entre PISEE y la API.

- **Balanceador de carga**:

    - Administra la distribución de las solicitudes hacia los diferentes nodos del cluster proveedor.
    - Asegura que el sistema sea escalable horizontalmente y se mantenga operativo incluso con altas cargas de trabajo.
    - **Tecnologías sugeridas**: Kubernetes, NGINX.

- **Servidor de monitoreo:**
    - **Monitoreo de servicios:** Permite identificar servicios caídos o con alta utilización de recursos. Este monitoreo es el que genera la alerta de escalamiento o de aumento de recursos en la infraestructura.
    - **Monitoreo de nodos:** Corresponde al servicio de monitoreo de los servicios provistos por OAE proveedoras de fuentes de información. Este monitoreo permite identificar caídas en los endpoints disponibles por las OAE.

- **Servidores APP (Servidor APP 2, Servidor APP n, etc.)**:
    - Ejecutan las aplicaciones y servicios encargados de manejar las solicitudes entrantes de los consumidores.
    - Es quien construye la ficha en base a la lógica de negocios definida.
    - Incluyen lógica de negocio y validación de datos.
    - **Tecnologías sugeridas**: Docker, lenguajes de programación como .NET, PHP, Java, Python.

- **Caché Centralizado**:
    - Reduce la carga sobre las bases de datos almacenando temporalmente los datos más solicitados.
    - Mejora significativamente la latencia y el rendimiento del cluster.
    - El caché centralizado puede funcionar como caché en memoria RAM y también en Disco, tiene configurado un ciclo de vida acotado de los datos.
    - El caché busca almacenar, temporalmente, la respuesta a las peticiones de cada servicio solicitado a las OAE para un rut en particular. El caché elimina la necesidad de repetir peticiones a los endpoints de los OAE si estas ya fueron realizadas.
    - Considerar un tiempo de expiración del caché de cada fuente de información.
    - **Tecnologías sugeridas**: Redis, Memcached, GraphQL.

- **Bases de Datos**:
    - **Base de datos transaccional**:
        - Almacena datos críticos en tiempo real, permitiendo escrituras frecuentes y actualizaciones.
        - Almacena todas las configuraciones administrativas de la plataforma (usuarios, roles, configuraciones de fuentes de datos, etc).
        - Esta es la base de datos que administra la gobernanza de la plataforma.

    - **Base de datos de solo lectura**:
        - Optimizada para consultas de lectura.
        - Contiene datos históricos o replicados para consultas masivas.
        - Contiene datos provenientes de cargas masivas y con un procesamiento ya realizado.
        - Los datos también tienen un ciclo de vida.

    - **Catálogo de Eventos**
        - Corresponde a una base de datos que almacena los eventos que pueden consumir las OAE.
        - Contiene también los eventos activos y notificaciones activas en el momento.
- **Sistema de Archivos**:
    - Gestiona los documentos, logs y respuestas generadas por las aplicaciones del cluster proveedor.
    - **Tecnologías sugeridas**: CephFS, MinIO, S3.
- **Servidor web**
    - **Plataforma del ciudadano:** Corresponde a la plataforma que disponibiliza la ficha del ciudadano desde una página web. Esta plataforma requiere acceso con clave única.
    - **Plataforma del funcionario:** Corresponde a una plataforma que le permite a los funcionarios visualizar información de algunos ciudadanos con motivo de la realización de algún procedimiento administrativo.
    - **Plataforma de administración:** Plataforma que permite la configuración de los distintos roles de usuarios en la plataforma, junto a proveer herramientas de monitoreo y configuración de las distintas fuentes de información. El acceso a esta plataforma es con clave única y con algún mecanismo de autenticación multifactor (MFA).
    - **Mesa de ayuda con IA:** Plataforma de soporte y respuesta de preguntas realizadas por los usuarios. Esta plataforma debe contener una base de conocimiento de los procedimientos administrativos y de las fuentes de información. Cumple un rol de apoyo a los ciudadanos y a los funcionarios.
    - **Observatorio de datos:** Plataforma de visualización de métricas relevantes en el sector laboral y previsional. Las métricas deben permitir la toma de decisión de distintos actores como lo son las universidades, OAE, fundaciones y empresas privadas del rubro.
- **Servidor privado**
    - Servidor que disponibiliza una API a instituciones privadas. Similar al servidor PISEE ficha, con la diferencia que las instituciones privadas no pueden acceder a nodos PISEE.
    - Las instituciones solo podrán acceder a fuentes de información particulares, las cuales son previamente configuradas para su acceso y a la cual se llegó a convenio.
    - Las instituciones deben disponibilizar la ip desde donde van a consumir la fuente de información. Esto para evitar accesos no autorizados.

5.2.2. Cluster Consumidor

Este subcomponente es el encargado de recibir solicitudes de los OAEs consumidores y proporcionarles los datos procesados por el cluster proveedor.

- **Balanceador de carga**:
    - Similar al cluster proveedor, este balanceador gestiona la distribución de solicitudes hacia los nodos ETL (Extract, Transform, Load).

    - **Tecnologías sugeridas**: Kubernetes Ingress, Envoy Proxy, Pentaho Data Integration, Python.
- **Nodos ETL (Extract, Transform, Load)**:
    - Corresponden a la capa de transformación y normalización.
    - Realizan el procesamiento de datos necesario para adaptar la información al formato requerido por los consumidores.
    - Contiene las lógicas de negocio preestablecidas para consumir los datos, procesarlos y disponerlos.
    - Estos servicios buscan consumir las fuentes de información de las distintas OAE y disponibilizarlos en la ficha. Se define que no modificarán la data provista por las OAE si no que se seleccionan los atributos de dichas fuentes que se entregarán en la ficha.
    - Esta componente también tiene un rol de validación de las fuentes de información y que cumplan con los criterios establecidos.
    - **Extract**: Obtiene datos desde el cluster proveedor o el caché centralizado.
    - **Transform**: Aplica validaciones, reglas de negocio y reestructuración de datos.
    - **Load**: Inserta los datos transformados en los sistemas internos de los OAEs consumidores.

5.2.3. Cluster Pub/sub

- **Servidor PISEE Pub/sub:**
    - Corresponde al servidor que disponibiliza el endpoint de la publicación y consumo de eventos del nodo laboral y previsional. Este tiene escalamiento vertical y cumple la función de middleware entre PISEE y el broker de eventos.
- **Balanceador de carga:**
    - Administra la distribución de las solicitudes hacia los diferentes brokers de eventos, ya sean para publicar o consumir los eventos.
    - Asegura que el sistema sea escalable horizontalmente y se mantenga operativo incluso con altas cargas de trabajo.
    - **Tecnologías sugeridas**: Kubernetes, NGINX.

- **Broker de eventos:**
    - Corresponden a la componente tecnológica que tiene la lógica de los eventos que se pueden consumir / suscribir o bien publicar.
    - Existe una gobernanza de los eventos (no todas las OAE pueden ver todos los eventos).
    - Los eventos pueden estar relacionados a la existencia de valores de una fuente de información de un ciudadano en particular, a eventos relacionados con la disponibilización de actualizaciones de endpoints completos (por ejemplo, se encuentra disponible el libro de remuneración de un mes en particular) o bien a notificaciones de caídas y recuperaciones de ciertas fuentes de información provistas por OAE productoras.

5.2.4 Otros Servicios del Cluster

Además de los subcomponentes principales, el Cluster de Interoperabilidad cuenta con un Firewall como un servicio auxiliar escencial, el cual tiene las siguientes funciones

- Controla el acceso a los recursos internos del cluster.
- Garantiza que las solicitudes externas sean seguras y que el tráfico entre los OAEs y el cluster esté protegido.
- **Tecnologías sugeridas**: iptables, OpenWrt o una solución de firewall en la nube (p.ej., WAF en AWS o Azure).

Para complementar la descripción de la infraestructura y facilitar su comprensión operativa, se incluye en el Anexo 2 un diagrama BPMN que detalla de forma gráfica el flujo y proceso para utilizar la solución descrita.

5.3. TIEMPOS DE RESPUESTA

El tiempo de respuesta esperado en este tipo de infraestructura dependerá de varios factores, por lo que se entrega una estimación basada en los rangos de tiempos óptimos para la respuesta en cada componente, según los umbrales establecidos en el mercado.

5.3.1. COMPONENTES Y ESTIMACIÓN DE LATENCIAS

A continuación, se muestran los tiempos en milisegundos (ms) de respuesta entre componentes, donde la conexión se explica por la flecha entre componentes, es decir, “componente 1”→”Componente 2”.

Caso 1 - Datos en caché ó base de datos:

1. **Nodo (consumidor) → Servidor PISEE (Llamada API entre servidores)**
    - Latencia típica: 10 - 50 ms
2. **Servidor PISEE → Balanceador de carga (Redirección de la consulta)**
    - Latencia típica: 5 - 30 ms
3. **Balanceador de carga → Servidor APP “n” (Distribución de carga y reenvío)**
    - Latencia típica: 5 - 30 ms (según la optimización del balanceador).
4. **Servidor APP “n” → Caché centralizada (Recuperación de datos de la caché)**
    - Latencia típica: < 10 ms (muy rápida si la caché está optimizada y cerca del servidor).

5. **Si los datos no están en la caché → Servidor APP "n" → Base de datos (Consulta y recuperación de datos)**
    - Latencia típica (consultas rápidas): 5 - 50 ms.
    - Latencia típica (consultas complejas o con alta carga): 50 - 300 ms.
    - Si la base de datos está optimizada, las consultas rápidas pueden devolver resultados en menos de 50 ms.
6. **Servidor APP "n" → Balanceador de carga → Servidor PISEE → Nodo (consumidor) (Retorno de la respuesta)**
    - Latencia típica: 20 - 100 ms (dependiendo de la optimización).

Tiempo total de respuesta esperado

Esto representa el tiempo de respuesta del sistema interoperable a la petición del entorno consumidor y todos los procesos anteriormente mencionados.

Escenario Óptimo - "Con datos en caché":

- **Escenario óptimo**: Si los datos están en la caché, el tiempo de respuesta podría ser de 50 - 100 ms. (Nodo Consumidor → Servidor PISEE → Balanceador de carga → Servidor APP "n" → Caché)

Escenario Promedio - "Sin datos en caché" (requiere búsqueda en base de datos):

- Si los datos no están en la caché y el sistema tiene que consultar la base de datos, el tiempo de respuesta podría ser de 200 - 600 ms. (Nodo Consumidor → Servidor PISEE → Balanceador de carga → Servidor APP "n" → Base de datos → Balanceador de carga → Servidor PISEE → Nodo Consumidor)

Escenario Pesimista - "Alta carga":

- En situaciones donde hay alta carga en la base de datos o las consultas son muy complejas, el tiempo de respuesta podría llegar a 600 ms - 2 s o más.

Caso 2 - Ejecución ETL

Considerando un escenario con 10 millones de registros, los tiempos de respuesta aproximados deberían ser los siguientes:

1. **Extracción (Extract)**:
    - El tiempo de extracción dependerá de la fuente de los datos. Si se trata de una base de datos o una API.
    - **Estimación de latencia**: **2 s - 10 s** (depende de la base de datos, la conexión y la optimización del sistema). Si la extracción proviene de una fuente externa o una base de datos no optimizada, el tiempo podría aumentar más.
2. **Transformación (Transform)**:
    - **Estimación de latencia**: **10 s - 1 min**, dependiendo de la complejidad de las transformaciones. Las operaciones de agregación, cálculos o joins con datos masivos pueden ser muy lentas, especialmente si no se paralelizan.
3. **Carga (Load)**:
    - Después de la transformación, los datos deben ser cargados en una base de datos o en un sistema de almacenamiento.
    - **Estimación de latencia**: **5 s - 30 s**, dependiendo de la base de datos y si tiene índices adecuados, particionamiento o es un sistema distribuido.

5.3.2. FACTORES QUE OPTIMIZAN EL TIEMPO DE RESPUESTA:

1. **Caché centralizada:** Si los datos más consultados están en caché, las respuestas serán extremadamente rápidas. Mantener la caché sincronizada con la base de datos es esencial para evitar consultas a la base de datos en cada solicitud.
2. **Optimización de base de datos:** Consultas indexadas y bien optimizadas, además de la utilización de particionamiento o bases de datos NoSQL en algunos casos, pueden mejorar significativamente el tiempo de respuesta.
3. **Balanceador de carga eficiente:** Usar un balanceador de carga que distribuya las consultas de manera eficiente entre varios servidores puede reducir los cuellos de botella y mejorar la velocidad de respuesta.
4. **Conexiones persistentes y tecnologías como HTTP/2 o gRPC:** Para evitar el overhead de establecer nuevas conexiones, el uso de conexiones persistentes (Keep-Alive) o protocolos más eficientes como gRPC puede reducir la latencia.
5. **Caché distribuida:** Si la caché es distribuida y geográficamente cercana a los usuarios, la latencia puede ser aún más baja.

5.4. Guía conexión con Nodo PISEE

El Nodo PISEE es una aplicación de software que funciona como middleware, facilitando el intercambio seguro de datos entre distintos Órganos de la Administración del Estado (OAE). Como parte del proyecto de diseño de este sistema interoperable, se realizó la instalación de un nodo en PISEE. En base al ejercicio anterior, se entrega la siguiente guía, donde se detalla el proceso de instalación y configuración del Nodo de manera local, permitiendo tanto el consumo como la provisión de datos.

Paso 1: Requisitos para comenzar la instalación.

Para la instalación se requieren dos servidores:

- **Servidor 1**: Consumidor.
- **Servidor 2**: Proveedor.

Especificaciones recomendadas:

- **Sistema operativo**: Compatible con Windows y Linux. Se recomienda utilizar un SO con el que el equipo tenga experiencia. Para esta guía, se usará **Ubuntu 24.04.2 LTS**.
- **Memoria RAM**: No hay un requisito específico, pero se recomienda un mínimo de **4GB**.
- **Almacenamiento**: **20GB**.
- **Procesador**: **2 Cores**.

Paso 2: Configuración de servidores:

Nodo "Consumidor":

- Es necesario habilitar el puerto **8084** para la entrada de mensajes.

- No es necesario exponerlo a Internet si las aplicaciones que consumen están en el mismo servidor. En caso contrario, sí debe ser expuesto.

Nodo "Proveedor":

- Puerto: **8489** (entrada de mensajes desde el exterior de la institución).

También es necesario que habilitar IP's y DNS, dependiendo del ambiente en el que se encuentren:

- Dirección ambiente de desarrollo

```
http://18.237.240.119:8500
```

```
http://18.237.240.119:8444
```

Dirección ambiente de producción

```
catalogo.pisee.cl:8500
https://server.pisee.cl:8444
```

Paso 3: Obtener aplicación Nodo.

Para obtener la aplicación, es necesario solicitarla al equipo PISEE. Tras la primera solicitud, la configuración podrá realizarse de manera autónoma. El equipo PISEE entregará una aplicación preconfigurada con credenciales y certificados necesarios para una conexión segura entre Nodos.

Paso 4: Instalación Nodo (distribución Linux)

Para iniciar la instalación del Nodo, se actualizarán los paquetes de la distribución Linux para prevenir errores relacionados con versiones antiguas. Cabe destacar que el proceso de instalación es el mismo tanto para el Nodo consumidor como para el Nodo proveedor.

```
sudo apt-get update
```

El siguiente comando debe ejecutarse únicamente si es necesario utilizar los servicios de SRCeI:

```
sudo apt-get install xmlsec1
```

Después de esto, se debe descomprimir el contenido del archivo enviado por el equipo de PISEE, el cual probablemente sea un archivo .rar o .zip. Para ello, es necesario que el servidor tenga instalado el paquete **unrar** o **unzip**, según corresponda. Se recomienda realizar este procedimiento en la carpeta **/var/www** del servidor. Los comandos para llevar a cabo esta acción son los siguientes:

Caso “.zip”:

```
sudo apt-get install unzip

#para descomprimir
unzip archivo.zip
```

Caso ".rar":

```
sudo apt-get install unrar

#para descomprimir
unrar x archivo.rar
```

Una vez descomprimido el archivo, se deben otorgar permisos de ejecución a la aplicación.

```
sudo chmod +x ./Nodo
```

Después de otorgar los permisos, también es necesario agregar los certificados **cert.pem** y **key.pem** (proporcionados por el equipo de PISEE) correspondientes para establecer una conexión segura. Estos certificados deben copiarse dentro de la carpeta **/certsX509** del aplicativo. Luego, se debe configurar el archivo **config.json**, ubicado en la carpeta principal del aplicativo, y agregar las claves correspondientes al organismo:

```
 "SRCeI": {
       "X509": {
            "privado": "./certsX509/key.pem",
            "publico": "./certsX509/cert.pem"
       }
   }
```

Con esto, la configuración debería estar completa y solo quedaría ejecutar la aplicación con el siguiente comando:

```
./NodoV2 start
```

Al ejecutar el comando, se mostrará un log como el siguiente:

Esto significa que ya está conectado al Nodo central. Este proceso debe dejarse tal como está (se puede cerrar el terminal). Si es necesario ejecutar un nuevo comando, se debe abrir otra terminal.

Paso 5: Probar conexión:

Para realizar una prueba de conexión, se debe ejecutar un comando **curl** a un Nodo de prueba, de la siguiente manera:

```
curl -X GET http://localhost:8084/detalleOrganismo/PE-SUB-00053
```

Esto debería responder con un JSON como el siguiente:


```
  {
     "id": 53,
     "codigo": "PE-SUB-00053",
     "descripcion": "Subsecretaría de Hacienda",
     "fecha_inicio": "2021-12-14T11:39:58.649389Z",
     "fecha_fin": "2999-12-30T21:00:00-03:00",
     "IdCodificacion": 1,
     "info_extra": "",
     "padre": 537,
     "id_codigo_padre_jerarquico": 0,
     "secuencia": 53,
     "fecha_cambio": "0001-01-01T00:00:00Z",
     "identificador": "1.PE-SUB-00053",
     "vigente": true
   }
```


¿Cómo consumir un nuevo servicio?

Se deben solicitar permisos al proveedor del nuevo servicio a consumir y modificar nuevamente el archivo **config.json**, agregando el nuevo servicio que se va a consumir.

```
"consumidor": [
{
   "nombre": "<Servicio en Catálogo>",
   "rutaLocal": "/test/nombreInterno"
}
```

Los servicios se pueden encontrar en el portal de PISEE, accediendo a la siguiente URL:

https://portal.pisee.cl/dashboard/catalogo

¿Cómo proveer datos con un servicio?

Se debe enviar la información correspondiente al equipo encargado de PISEE para que

publique este nuevo servicio. Los datos a enviar son los siguientes:

- La IP o DNS del Nodo que va a exponer el servicio.
- El puerto por el cual se va a exponer el Nodo hacia Internet (en el config.json está en la sección puerto->externo, por defecto 8489).
- El valor que se colocó en “rutaExterna”.
- Se solicita también un ejemplo de cómo llamar el servicio (si es con path params o un POST con body), esto es necesario para enviarlo como documentación a los consumidores al momento de habilitarlos.

Una vez realizado este proceso, se debe editar el archivo **config.json** y, en la sección **proveedor**, agregar el siguiente script:

```
"proveedor": [
  {
      "nombre": "<NombreDelServicioSegunElCatalogo>",
      "origen": {
            "tipo": "WEB_SERVICE",
            "rutaLocal": "http://ip/ruta_local/servicio"
      },
      "rutaExterna": "/nombreServicio",
      "tps": <n>
  }
```

En algunas ocasiones, cuando se agrega un nuevo servicio, es necesario reiniciar o limpiar la base de datos local del aplicativo del Nodo. Por lo tanto, se recomienda ejecutar el siguiente comando:

```
./NodoV2 clean
```

En la siguiente tabla se pueden ver los comandos disponibles para el aplicativo, junto con un resumen de lo que hacen:

Comandos para Nodo habilitado

Comando	Descripción
`./NodoV2 start`	Inicia el Nodo de Interoperabilidad
`./NodoV2 stop`	Detiene el Nodo de Interoperabilidad
`./NodoV2 version`	Muestra la versión del Nodo
`./NodoV2 autoevaluacion`	Efectúa una evaluación de accesos y permisos
`./NodoV2 estado`	Muestra indicadores del estado de ejecución del Nodo
`./NodoV2 certificados`	Lista todos los certificados cargados
`./NodoV2 certificados <id_organismo>`	Muestra el detalle de los certificados de un organismo
`./NodoV2 certificados --descarga`	Obliga al nodo a efectuar una recarga forzada de los certificados
`./NodoV2 servicios`	Lista los servicios configurados
`./NodoV2 servicios <nombre_servicio>`	Muestra el detalle de un servicio y sus estadísticas de uso más reciente
`./NodoV2 trazabilidad`	
`./NodoV2 clean`	Limpia la base de datos local del Nodo, lo cual obliga al Nodo a volver a cargar los certificados de las contrapartes y los endpoints de los servicios con los cuales interopera.

6. GESTIÓN DE LAS FUENTES DE DATOS

6.1. TECNOLOGÍA USADA POR LAS OAES PARA ALMACENAR, DISPONIBILIZAR Y COMPARTIR DATOS

Los Órganos de Administración del Estado (OAEs) utilizan tanto soluciones on-premise como en la nube, cada una con ventajas y desventajas dependiendo de las necesidades de cada organismo.

Las tecnologías on-premise ofrecen ventajas como menor dependencia de terceros y mayor control sobre los recursos, lo que permite una gestión directa de la infraestructura. Además, al estar localizadas, suelen tener menor latencia y tiempos de respuesta más rápidos. Sin embargo, requieren una inversión inicial significativa, personal especializado y tienen una escalabilidad limitada, ya que dependen de la capacidad física instalada.

Las soluciones en la nube, por otro lado, destacan por su escalabilidad y flexibilidad, permitiendo a los OAEs ajustar recursos de almacenamiento y procesamiento según las demandas cambiantes. Pueden escalar vertical u horizontalmente, adaptándose rápidamente sin necesidad de grandes inversiones en infraestructura física. Esto permite reducir los costos iniciales (CAPEX) y optimizar los gastos operativos (OPEX), ya que las organizaciones solo pagan por los recursos utilizados.

Sin embargo, esta infraestructura también tiene desventajas. La dependencia del proveedor puede ser un riesgo, ya que las organizaciones quedan sujetas a las condiciones y capacidades del proveedor, lo que puede dificultar la migración a otros proveedores o infraestructuras locales. Además, el rendimiento y la latencia pueden verse afectados por la ubicación de los centros de datos del proveedor y la calidad de la red, lo que podría resultar en tiempos de respuesta más largos o variabilidad en el rendimiento durante picos de demanda.

Además de la infraestructura empleada, las fuentes de datos utilizadas por los OAEs presentan características diversas en cuanto a su tipología y formato. Estas pueden ser de naturaleza transaccional, provenir de web services, o distribuirse mediante archivos alojados en servidores FTP. Los formatos de los datos incluyen JSON, XML y archivos planos como CSV o excel, dependiendo del propósito y la tecnología asociada a cada fuente. Estas características extraídas del levantamiento realizado con las OAEs, serán detalladas en las siguientes secciones, junto con el análisis de las tecnologías empleadas por las fuentes de datos para la Ficha Única.

OAE	Fuente de dato	Infraestructura	Tipo	Formato	Tipos de datos a compartir

IPS	obtenerresolucionAF	Alojado en Azure	WS PISEE 2.0.	JSON	Data transaccional
IPS	ProximaFechaPagoBeneficios	Alojado en Azure	WS PISEE 2.0.	JSON	Data transaccional
SUSESO	ConsultaAfiliacionMutual	Nube Nutanix (infraestructura hiperconvergente)	PISEE 2.0.	JSON	Data transaccional
SUSESO	ConsultaAfiliacionCaja	Nube Nutanix (infraestructura hiperconvergente)	PISEE 2.0.	JSON	Data transaccional
SUSESO	SIAGFConsultaCausanteSimple	Nube Nutanix (infraestructura hiperconvergente)	PISEE 2.0.	JSON	Data transaccional
DT	Registro de Contrato de Trabajo	Alojado on-premise	FTP	Archivo de texto plano	Archivo de texto plano CSV
DT	Registro de Término de Contrato de Trabajo	Alojado on-premise	FTP	Archivo de texto plano	Archivo de texto plano CSV
DT	Libro de Remuneraciones Electrónico	Alojado en Azure	FTP	Archivo de texto plano	Archivo de texto plano CSV
SP	Cotizaciones previsionales	Por definir	WS	JSON	Data transaccional

Se identifica que los mecanismos utilizados para compartir las fuentes de datos son dos: cargas masivas (FTP) y servicios web (WS). Ambos son fundamentales para el funcionamiento eficiente del sistema de interoperabilidad, ya que permiten una adecuada transferencia y disponibilidad de datos, aunque con enfoques distintos.

Las cargas masivas de datos permiten centralizar y almacenar grandes volúmenes de información clave de manera eficiente en el sistema de interoperabilidad. Este enfoque facilita la disponibilidad inmediata de la información para consultas futuras, optimizando significativamente los tiempos de respuesta. Al estar integrada en el sistema, la información no requiere realizar solicitudes externas en cada consulta, lo que mejora la velocidad y eficiencia del proceso.

Por otro lado, los datos transaccionales, obtenidos a través de servicios web (WS), implican un proceso más complejo y lento. En este caso, la información debe ser solicitada directamente a la institución propietaria, lo que puede generar retrasos debido al tiempo de respuesta de la consulta y la posterior transmisión de los datos entre las entidades. Este mecanismo, aunque más dinámico, puede resultar en cargas adicionales en los nodos de las redes, afectando la eficiencia en el manejo de consultas en tiempo real.

Es relevante señalar que, en el caso de los datos cargados a la plataforma mediante cargas masivas, estos no serán almacenados de manera indefinida. El sistema implementará mecanismos para eliminar la información que ya no sea relevante o necesaria para los

propósitos de interoperabilidad. Esto asegura que únicamente se mantenga aquella información que sea pertinente para las consultas y que cumpla con los marcos legales y regulatorios aplicables. De esta manera, se promueve una gestión eficiente de los recursos de almacenamiento y se respeta el compromiso con las políticas de privacidad y protección de datos, conforme a los acuerdos entre las instituciones participantes.

6.2. Convenios entre OAEs

Los Organismos Autónomos del Estado (OAEs) establecen convenios de intercambio de información con el objetivo de facilitar la interoperabilidad entre instituciones y garantizar que cada OAE pueda acceder a los datos requeridos de otras entidades o instituciones. Estos acuerdos deben ajustarse a la normativa vigente y definir de manera clara el propósito del intercambio, especificando los tipos de datos a compartir, las instituciones involucradas y las actividades autorizadas. A continuación, se detallan los convenios vigentes correspondientes a las fuentes de datos actualmente propuestas para la Ficha Única.

OAE	Fuente de dato	Demandante
IPS	obtenerresolucionAF	Chileatiende
IPS	ProximaFechaPagoBeneficios	Mindes SPS
SUSESO	ConsultaAfiliacionMutual	ISL IPS
SUSESO	ConsultaAfiliacionCaja	ISL IPS
SUSESO	SIAGFConsultaCausanteSimple	Por definir*
DT	Registro de Contrato de Trabajo	SII INE SENCE Banco Central SUBTRAB
DT	Registro de Término de Contrato de Trabajo	ChileValora ISL IPS SENCE SUBTRAB SUSESO
DT	Libro de Remuneraciones Electrónico	SENCE INE
SP	Certificado de cotizaciones previsionales	CAPREDENA CHVALORA ISL SENCE SPS SUBTRAB SUCESO

En este contexto, se recomienda que el sistema de convenios en el modelo de interoperabilidad, sustentado por el nodo sectorial, se transforme hacia un enfoque unificado en el sector. En lugar de acuerdos bilaterales individuales entre instituciones por cada dato, se debería establecer un convenio general que abarque las condiciones para el acceso, uso y protección de los datos en el marco del nodo sectorial. Este convenio establecería claramente los fines autorizados, las instituciones participantes y los datos involucrados, delegando en el nodo la gestión operativa y técnica de las transacciones[9].

[9] Cabe destacar que, aunque la recomendación posee un carácter fundamentalmente operativo, su implementación deberá contar con la validación legal que garantice el cumplimiento de la normativa vigente.

Este actuaría como intermediario, implementando controles de acceso centralizados basados en roles y asegurando que las solicitudes cumplan con las condiciones del convenio. Además, debe garantizarse la trazabilidad completa de las transacciones, registrando cada acceso para auditorías y control de cumplimiento. Este enfoque permite escalar el sistema, facilitando la incorporación de nuevas instituciones y datos, a la vez que refuerza la seguridad, transparencia y alineación con las normativas vigentes de protección de datos.

7. Ficha Única de información laboral y previsional

7.1. Convención de nomenclatura

Si bien, se ha comentado anteriormente sobre cómo se gestiona actualmente el envío de información entre los organismos del estado, las alianzas que existen y el formato de envío de esta información; la solución de la Ficha Única debe tomar en cuenta las diferentes estructuras y convenciones de nomenclatura/codificación con las cuales están diseñadas las fuentes de datos de cada OAE.

Por ejemplo, en las muestras de las siguientes fuentes de datos, se evidencia en el caso de IPS, SUSESO y SP que a pesar de tener el formato JSON en el envío de su información, aún hay diferencia en las convenciones de nomenclatura. Es decir:

- En el caso de IPS se usa una nomenclatura Camell Case (Ejemplo: `nombreCompleto`)
- SUSESO usa en la fuente de datos consulta causante simple Pascal Case (Ejemplo: `NombreCompleto`)
- SP evalúa el uso de la nomenclatura Snake Case (Ejemplo: `nombre_completo`)

Por otro lado, hay fuentes de datos que se envían en formato de archivo plano (en el caso de DT), por lo que se debe parametrizar las fuentes de datos que llegarán a componer la Ficha Única. Específicamente, la Ficha Única que se propondrá en la siguiente subsección, será enviada en el sistema interoperable bajo la nomenclatura Camell Case.

OAE	Muestra de datos por fuente	Formato

IPS	“ProximaFechaPagoBeneficios”:{
	"codigoRetorno": <código retorno>,
	"glosaRetorno": "<glosa retorno>",
	"idConsumidor": <idConsumidor>,
	"resultado": {
	"runBeneficiario": <runBeneficiario>,
	"dvBeneficiario": "<dvBeneficiario>",
	"proximoPago": {
	"FechaProximoPago": <FechaProximoPago>,
	"beneficio": “<beneficio>”,
	"formaPago": “<formaPago>”,
	"descripcionBeneficio": “<descripcionBeneficio>”
	}
	},
	"timestamp": "<marca de tiempo de cuando fue obtenida la información>"
	}
		JSON

SUSESO	RespuestaCausante: {
	"FechaEmision": "<fecha_emision>",
	"Tupla": [
	{
	"Causante": {
	"TipoCausante": {
	"CodTipoCausante": "<tipo_causante>",
	"NomTipoCausante": "<nombre_tipo_causante>"
	},
	"RutCausante": "<rut_causante>",
	"NomCausante": "<nombre_causante>",
	"SexoCausante": "<sexo_causante>",
	"FecNacCausante": "<fecha_nacimiento_causante>",
	"RegionCausante": {
	"CodRegionCausante": "<region_causante>",
	"NomRegionCausante": "<nombre_region_causante>"
	}
	},
	"Beneficiario": {
	"TipoBeneficiario": {
	"CodTipoBeneficiario": "<tipo_beneficiario>",
	"NomTipoBeneficiario": "<nombre_tipo_beneficiario>"
	},
	"RutBeneficiario": "<rut_beneficiario>",
	"NomBeneficiario": "<nombre_beneficiario>",
	"RegionBeneficiario": {
	"CodRegionBeneficiario": "<region_beneficiario>",
	"NomRegionBeneficiario": "<nombre_region_beneficiario>"
	}
	}
	}
	]
	}
		JSON

SP	{
	"certificado_cotizaciones_previsionales": {
	"rut": "TEXTO",
		JSON

	<pre>"nombres": "TEXTO",
	"apellidos": "TEXTO",
	"cotizaciones": [
	{
	"RUT AFP": "TEXTO",
	"periodo_cotizado": "yyyy-mm",
	"monto_cotizado_10": "numerico",
	"%cotizado": "numerico",
	"fecha_pago": "yyyy-mm-dd",
	"monto_remuneracion_imponible": "numerico",
	"tipo_movimiento": "TEXTO",
	"fondo_destino": "TEXTO",
	"rut_pagador_empleador": "TEXTO"
	}
	],
	"fecha_corte_afp": "yyyy-mm-dd"
	},
	"timestamp": "<marca de tiempo de cuando fue obtenida la información>"
	
	}</pre>	

DT	Los siguientes datos son algunos de los campos pertenecientes a la tabla que representa la fuente “Registro de Contrato de Trabajo”: IDContrato CategoriaContrato FechaSuscripcionContrato Rut_Empleador RUT_Trabajador Fecha_Nacimiento Nombres Apellidos Declaracion_Discapacidad Declaracion_Invalidez Funciones EstadoId Estado_Contrato Fecha_Inicio_Contrato"	Archivo Plano

7.2. Estructura de Ficha Única previsional y laboral

7.2.1. Petición

Para hacer solicitud de la Ficha Única al nodo sectorial, o del contenido específico dentro de esta, la OAE enviará la información contenida en el Header y el Payload mostrado en el ejemplo a continuación a través del método POST. Donde

- Header: se indica el tipo de contenido (permanentemente se mantendrá de esta forma dado que la ficha se entregará en este formato).
- Payload
    - **Operaciones:** Se especifican las fuentes de datos a solicitar dentro de la ficha en el formato "`Entidad.FuenteDeDato`". Esto es realizable dada la estructura modular que tiene la ficha con esta separación.
    - **Procedimiento** por el cual se le autoriza a la institución para solicitar la información, por parte del ciudadano dueño de la información (Online o Presencial).
    - **Token Clave Única:** token entregado por el ciudadano al solicitar información a una OAE por un medio online, donde este debe acceder con Clave Única.

      Por ejemplo, si el ciudadano entra al sitio de SUSESO "mi portal" con su clave, para iniciar un trámite que requiere sus 12 últimas cotizaciones (entregadas por SP), este puede solicitar a la OAE obtener esa información internamente. Para cumplir con lo anterior SUSESO solicitará la Ficha Única con la fuente de datos "`SP.ultimasCotizacionesPrevisionales`" y enviando el token de este para tener acceso a la información.
    - **CPAT:** Registro del código CPAT con el cual se asocia la solicitud de información a un tipo de transacción y entidad definida por CPAT.

```
URL: https://nodo.previsionsocial.cl/api/ficha/{rut}
RequestMethod: POST

Request Header: {
  "Content-Type": application/json*
}
Payload: {
    "operaciones": [
          "IPS.obtenerresolucionAF",
          "SP.ultimasCotizacionesPrevisionales"
     ],*
     "procedimiento": "<online|presencial>",*
     "tokenClaveUnica": "<TOKEN_CLAVE_UNICA_DEL_USUARIO>",**
     "cpat":"<Código CPAT>"*
 }
```

Los campos marcados con "*" serán obligatorios para poder acceder a la información de la Ficha Única tanto realizando el trámite presencialmente con el ciudadano, como online. Pero, para acceder a esta información sin la autorización presencial, se requerirá del token que entrega el ciudadano al solicitar los datos con la Clave Única (campo con "**").

En el siguiente ejemplo, se está solicitando al nodo sectorial la fuente de dato perteneciente a IPS “Resolución AF” (`"IPS.obtenerresolucionAF"`), el perteneciente a SP “ultimasCotizacionesPrevisionales” (`"SP.cotizacionesPrevisionales"`), y por último a SRCEI “datosBasicos” (`"SRCEI.datosBasicos"`).

Un elemento a destacar es que, a pesar de ser inicialmente una solución para las OAEs del Ministerio del Trabajo, los datos de identificación del ciudadano, deben ser corroborados con la fuente original de esta información (en este caso el Servicio de Registro Civil e Identificación o SRCEI).

```
#Ejemplo online
curl -X POST "https://nodo.previsionsocial.cl/api/ficha/18971801k"
\
  -H "Content-Type: application/json" \
  -d '{
        "OperacionesSolicitadas": [
          "IPS.obtenerResolucionAF",
          "SP.cotizacionesPrevisionales",
          "SRCEI.datosBasicos"
        ],
        "Procedimiento": "online",
        "TokenClaveUnica": "TOKEN_CLAVE_UNICA_DEL_USUARIO",
        "cpat":"TR-SUB00033-00022"
      }'

#Ejemplo presencial
curl -X POST "https://nodo.previsionsocial.cl/api/ficha/18971801k"
\
  -H "Content-Type: application/json" \
  -H "Authorization: Bearer <TOKEN_DE_AUTENTICACION>" \
  -d '{
        "operacionesSolicitadas": [
          "IPS.obtenerResolucionAF",
          "SP.certificado_cotizaciones_previsionales",
          "SRCEI.datos_basicos"
        ],
        "procedimiento": "presencial",
        "cpat":"TR-SUB00033-00022"
      }'
```

7.2.2. FICHA ÚNICA

En línea con el ejemplo anterior, la siguiente estructura representa la respuesta que enviaría el nodo sectorial de la Ficha Única con las 3 fuentes de datos solicitadas (para ver la versión con todas las fuentes de datos de las 4 OAEs iniciales, el Response Header y el Status report; revisar Anexo 5).

Cómo se mencionó en la subsección 7.2.1, la ficha mantendrá una nomenclatura Camell Case, ordenando los grupos de fuentes de datos por OAE, enviando modularmente cada fuente solicitada.

```
Response Header: {

  "Status": {
    "code": 200,
    "message": "OK - Solicitud exitosa",
  },

  "Content-Type": application/json
}

//respuesta json

{
  "FichaUnica":{

    "SRCEI": {
      "datosBasicos": {
        "nombres": "STRING",
        "apellidos": "STRING",
        "rut": "STRING",
        "fechaNacimiento": "DATE(YYYY-MM-DD)",
        "comuna": "STRING”
      }
    },
    "IPS": {
      "obtenerResolucionAF": {
        "solicitudId": "NUMERIC",
        "beneficioId": "NUMERIC",
        "descripcion": "STRING",
        "idRepositorio": "NUMERIC",
        "idRepositorioFinal": "NUMERIC",
        "fecCreacionAno": "NUMERIC",
        "fecCreacionMes": "NUMERIC",
        "base64File": "BLOB",
        "timestamp": "DATETIME()"
```

```
      }
    },
    "SP": {
      "cotizacionesPrevisionales": {
        "fechaUltimaCotizacion": "DATE(YYYY-MM-DD)",
        "cotizaciones": [
          {
            "rutAfp": "STRING",
            "periodoCotizado": "DATE(YYYY-MM)",
            "montoCotizado": "NUMERIC",
            "porcentajeCotizado": "NUMERIC",
            "fechaPago": "DATE(YYYY-MM-DD)",
            "montoRemuneracionImponible": "NUMERIC",
            "tipoMovimientoCotizacionObligatoria": "STRING",
            "fondoDestino": "STRING",
            "rutPagadorEmpleador": "NUMERIC"
          }
        ],
        "fechaCorteAfp": "DATE(YYYY-MM-DD)"
      }
    }
  },
  "serviceStates": {
    "SRCEI": {
      "datosBasicos":{
        "code": 200,
        "message": "OK - Solicitud exitosa",
      }
    },
    "IPS":{
      "obtenerResolucionAF":{
        "code": 200,
        "message": "OK - Solicitud exitosa",
      }
    },
    "SP":{
      "ultimasCotizacionesPrevisionales":{

        "code": 200,
        "message": "OK - Solicitud exitosa",

       }
    }
```

7.2.3. STATUS CODE

Como se mencionó anteriormente, el Response Header entrega un estado de las fuentes de datos entregadas a través de un código y un mensaje asociado.

```
Response Header: {
    "Status": {
     "code": 200,
     "message": "OK - Solicitud exitosa",
   },
   "Content-Type": application/json
}
```

Apoyándose en los *Status-Code* comúnmente utilizados en soluciones tecnológicas, se proponen los siguientes, con su significado asociado al sistema interoperable:

Status code	**Significado**
200	OK - Solicitud completamente exitosa exitosa
207	MultiStatus - Algunas fuentes fueron exitosas y otras no
400	Bad Request - JSON mal formado o datos inválidos
401	Unauthorized - No autorizado para acceder al recurso de alguna de las fuentes
429	Too Many Request - Se ha sobrepasado la cantidad de solicitudes por segundo permitidas
503	Service Unavailable - Servicio no disponible

La mayoría de estos códigos representan situaciones booleanas, se puede entregar o no la ficha como tal. En cambio, en el caso que hayan fuentes a las que sí se pudieron acceder a través de la petición pero el resto de ellas no se entregaron de forma expedita, o simplemente no fueron entregadas, se enviaría información incompleta.

Por lo que, para que el usuario del sistema pueda abordar esta situación, se entrega un código general de la ficha “207” de *Multistatus* (informando que hay respuestas distintas para los estados de cada fuente de datos), además se incorpora al final de la ficha el apartado de Status para cada fuente de dato (`"serviceStates": {}`). Los *status* de las respuestas de cada fuente de información, tienen los siguientes valores disponibles de estatus.

Code	Significado
200	OK - Solicitud exitosa
400	Bad Request - Datos inválidos
401	Unauthorized - No autorizado para acceder al recurso
403	Forbidden - Acceso prohibido
404	Not Found - Recurso no encontrado
500	Internal Server Error - Error interno del servidor (incluye envío incorrecto de datos)
503	Service Unavailable - Servicio no disponible
504	Gateway Timeout - Tiempo de espera agotado

En el mismo ejemplo comentado a lo largo de la sección, se muestra el código “200” en el *status* del *Response Header*.

8. Riesgos del sistema y su mitigación

Dentro de los potenciales riesgos en el desarrollo e implementación del sistema propuesto se identifican desafíos tanto técnicos como operativos. A continuación, se presenta el detalle de cada área de riesgo identificada, junto a sus respectivas acciones de mitigación.

8.1. Riesgos técnicos

Se consideran como riesgos técnicos aquellos relacionados con la tecnología a implementar lo cual puede comprometer el funcionamiento, rendimiento y seguridad del sistema propuesto.

8.1.1. Único punto de fallo

Al existir tener un único lugar donde las OAE consuman información laboral y previsional, significa un riesgo ya que si el nodo se encuentra indisponible entonces todos los OAE del sector perderán los servicios digitales que dependen de la ficha(antes solo quedaba indisponible uno de varios, ya que no todos se caían, ahora estarán todos indisponibles).

Mitigación:

Distribuir el nodo en múltiples dimensiones:

1. **Redundancia de Data center:** Contar con respaldos y servicios del Datahub en varios proveedores distintos (AWS, Azure, GCP, OnPremise, etc.)
2. **Múltiples Instituciones a cargo:** El nodo podría ser administrado por más de un organismo del rubro.
3. **Redundancia de nodos:** Podrían existir dos nodos réplica, en infraestructura distinta, de tal manera que si cae uno, los OAE apunten al otro.

8.1.2. Calidad de los datos

En esta categoría se consideran desafíos asociados a datos incompletos, duplicados, inconsistentes o que sean inaccesibles en los sistemas actuales. Es un riesgo que se incluyan fuentes de datos que generen inconsistencias entre ellas, por ejemplo, se observan múltiples fuentes de datos que podrían indicar distintos sueldos imponibles de un trabajador (la Dirección del Trabajo tiene Previred, la SUSESO con las mutuales, y el SP con las AFP).
Otro riesgo técnico asociado a la calidad de los datos es que el Datahub informe datos erróneos debido a que algún OAE informe, algún dato incorrecto y luego lo corrija posterior a ser informado por el Datahub.

Mitigación:

Para abordar esta problemática se recomienda implementar un modelo de gobernanza de datos que defina las estructuras formales sobre políticas, estándares, reglas de validación y calidad de datos, que permita definir qué institución informa el dato, con qué fecha y la validez y que se informen los distintos datos para que el OAE que los consuma defina la lógica de negocios con la que lo procesa (que las OAE definan qué remuneración imponible utilizar).

Además, se debe tener una log de transacciones que almacene las peticiones y respuestas de cada solicitud al Datahub, esto con el fin de permitir una auditoría de los datos entregados a los distintos OAE. El log de transacciones también se debe considerar como un activo de información el cual debe ser respaldado y contar con un ciclo de vida del dato. Cada transacción debe indicar la fecha y hora, el tiempo de respuesta, la petición de pregunta, la petición de respuesta y qué OAE lo solicitó.

La esencia del Datahub debe ser entregar datos con el menor procesamiento posible, de tal manera de disponer información lo más similar a lo entregado por la OAE que lo entrega.

8.1.3. Ciberseguridad

La exposición a ataques debido a la ampliación de los puntos de intercambio de información entre instituciones y las brechas de seguridad que existan en una o más instituciones podrían comprometer a toda la red interoperable.
Adicionalmente, el nodo puede ser susceptible a que los OAE carguen archivos o fuentes de información maliciosas debido a un hackeo, comprometiendo la integridad de los sistemas, facilitando la introducción de malware o la manipulación de datos.

Mitigación:

La arquitectura debe incorporar mecanismos robustos de seguridad, como autenticación mutua y encriptación TLS 1.3 y se debe diseñar controles robustos de seguridad, como cifrado de extremo a extremo (como los que provee PISEE 2.0) para todos los datos intercambiados, autenticación multifactor (MFA) y protocolos seguros de comunicación (como HTTPS, TLS). Además, se recomienda segmentar la red para reducir riesgos en caso de ataques y desarrollar un plan de acción para responder a estos, incluyendo la identificación, contención, erradicación y recuperación.

Quienes administren el nodo deben contar con políticas similares a la ISO 27.001 para abordar la ciberseguridad. Los servidores deben contar con sistemas operativos de larga duración de soporte y actualizados. Se deben realizar pruebas de seguridad (Pentesting u otros) de forma periódica. La plataforma debe contar con mecanismos de respaldos de información y simulacros de restauración.

Para mitigar los riesgos asociados a un hackeo se pueden aplicar una o más de las siguientes propuestas:

1. Aislar el procesamiento de los datos del OAE de los demás. Esto se puede lograr teniendo un servidor de procesamiento por OAE de tal manera que no se contaminen las distintas fuentes de información.
2. Aislar el procesamiento de datos del datahub. La idea es que el procesamiento de datos ocurra en servidores independientes al que consolida la ficha.
3. Incluir reglas de validación de cada fuente de información para verificar la estructura (que tenga los campos y tipos de datos correctos) y su contenido (que los valores vengan en rangos predefinidos). Para el caso de los archivos, solo se deben aceptar archivos que cumplan con los formatos predefinidos (por ejemplo la extensión del archivo y su nombre). Adicionalmente se debe examinar el archivo en modo de lectura (sin permiso de ejecución) y revisar que las cabeceras sean las correspondientes, al igual que los datos.
4. Cada error de validación del punto anterior debe generar una alerta y registrar un log para poder auditar dicho error.

8.1.4. Escalabilidad y desempeño

La infraestructura propuesta puede no ser lo suficientemente robusta para manejar volúmenes crecientes de datos o interacciones conforme se amplía el proyecto. Esto puede traducirse en mayores tiempos de respuesta, especialmente si los sistemas no están optimizados para grandes transacciones.

Mitigación:

Para garantizar que la infraestructura pueda manejar volúmenes crecientes de datos e interacciones, se debe diseñar un sistema con capacidad de escalamiento horizontal y vertical. Además, es crucial asegurarse de que los servidores y las bases de datos soporten altos volúmenes de transacciones, y realizar simulaciones con grandes cargas de datos para verificar el rendimiento en condiciones extremas. Implementar soluciones híbridas o en la nube puede ayudar a cubrir necesidades de escalabilidad de almacenamiento y procesamiento, siempre asegurando el cumplimiento con normativas de soberanía digital y privacidad.

Por otra parte, la carga debe ser distribuida entre los proveedores del Datahub en caso de ser más de uno. Además, se deben hacer pruebas de rendimiento periódicas, junto con simulacros para disminuir los tiempos de respuesta ante eventualidades.

Adicionalmente, se propone la incorporación de un sistema de caché para minimizar las peticiones a los Organismos de Administración del Estado. Se espera que este no solo reduzca la carga en los sistemas de las OAE, sino que también mejore el tiempo de respuesta del sistema global, optimizando el uso de recursos. Al reducir las peticiones directas a las OAE, se libera capacidad de procesamiento que puede ser utilizada para integrar nuevas instituciones o manejar un aumento en la carga de manera más eficiente.

8.1.5. Riesgo de adopción

Para quienes consuman información del nodo, puede suceder que los OAE no tengan las capacidades técnicas para desarrollar las piezas de código que consumen el nodo laboral y previsional.

En el caso de los productores de información pueden existir complicaciones dado que algunos OAE no tengan capacidades técnicas o recursos (infraestructura) para disponibilizar la información al Nodo.

Mitigación:

Para abordar el problema de los consumidores de información, se recomienda que al inicio del proyecto se provean proveer los scripts consumidores del nodo junto con documentación de cómo instalarlo a los OAE, los pasos a paso a seguir, el troubleshooting, etc. facilitando el proceso de implementación en las instituciones usuarias, teniendo en consideración cuáles tienen mayores riesgos de adopción dado su nivel de madurez tecnológica. Para esto se recomienda ejecutar un plan de migración progresiva de servicios y que considere la adopción de capacidades por fase con reutilización de componentes e implementación de soluciones preconfiguradas. ..

Respecto a los productores, el Datahub debe tener la capacidad de recibir fuentes de información como carga masiva (con almacenamiento) y de encargarse de disponibilizar la información al sector.

8.2. Riesgos operativos

Este tipo de riesgos se relacionan con los procesos cotidianos y su interacción con los servicios interoperables.

8.2.1. Fallas en la continuidad del servicio

Al depender excesivamente de una infraestructura interoperable puede que un fallo interrumpa múltiples sistemas en cascada.

Mitigación:

Quien administre la plataforma debe contar con un plan de continuidad de negocio que permita abordar los escenarios de caídas del servicio.

En primer lugar, se recomienda realizar simulaciones con grandes cargas de datos que permitirán verificar el rendimiento del sistema bajo condiciones extremas, asegurando que pueda manejar eficientemente volúmenes significativos de información sin comprometer su funcionalidad.

Además, se sugiere configurar arquitecturas de alta disponibilidad, incluyendo la implementación de clusters redundantes y el uso de balanceo de carga, con el fin de evitar interrupciones críticas en el servicio, garantizando que el sistema continúe operando incluso en caso de fallos en uno o más componentes.

Por último, se establece la necesidad de implementar mecanismos de respaldo de datos y código. Esto implica la programación de backups regulares y la definición de políticas claras de recuperación y el desarrollo de planes de continuidad operativa que permitan restaurar los servicios rápidamente en caso de fallos. Estas medidas pueden incluir la replicación de datos en tiempo real y la migración automática entre servidores, asegurando así la integridad y disponibilidad continua de la información.

8.2.2. Pruebas y gestión de cambios

La falta de pruebas rigurosas antes de la integración puede derivar en fallos inesperados tras la puesta en marcha.

Mitigación:

Toda nueva funcionalidad debe ser trabajada en ambientes de desarrollo y pruebas similares a los ambientes productivos de tal manera de minimizar los efectos adversos causados por dependencias de software. Se debe contar con un ambiente de staging o preproductivo el cual sea un clon del ambiente productivo y que sirva para simular el paso a producción. Esto permitirá probar la solución en el ambiente productivo y verificar que no existirán errores al hacer el paso a producción.

8.2.3. Registro de trazabilidad

Si no se asegura la integridad de estos registros, podría haber discrepancias en el seguimiento de las operaciones, lo que afectaría la transparencia, rendición de cuentas y procesos de auditoría.

Mitigación:

Se propone implementar un sistema de trazabilidad que capture y almacene metadatos de cada transferencia de información de manera automática y segura. Este debe registrar elementos clave como la fecha y hora exacta de la transferencia, el origen y destino de la información, el usuario o sistema que realiza la solicitud, el tipo de operación ejecutada y su resultado. Además, los registros deben ser inmutables y almacenarse en una base de datos segura con respaldos periódicos, implementando mecanismos de firma digital o hash criptográfico para garantizar que no han sido alterados. Además, el sistema debe contar con capacidades de búsqueda y recuperación eficiente para facilitar auditorías y la resolución de incidentes.

8.3. RIESGOS LEGALES

En el contexto de la implementación del sistema propuesto se identifican dos riesgos legales significativos. El primero se relaciona con la potencial resistencia de las Organizaciones de la Administración del Estado (OAE) a compartir información con otras instituciones, lo que podría limitar severamente la efectividad del sistema interoperable. El segundo riesgo corresponde a posibles cambios en el marco regulatorio y legislativo que podrían afectar los procesos y requerimientos establecidos para el sistema.

Mitigación:

Para abordar la resistencia institucional, se recomienda establecer convenios formales de colaboración entre instituciones e implementar un marco de gobernanza claro que defina roles, responsabilidades y protocolos de intercambio de información. La plataforma debe poder segmentar la información según OAE consumidora, de tal manera de no compartir toda la información con todos.

En cuanto a los cambios regulatorios, es fundamental diseñar la solución con una arquitectura flexible y adaptable, incluyendo en los contratos con proveedores la obligación de realizar los ajustes necesarios para mantener la conformidad legal, además de establecer procesos de monitoreo continuo de cambios regulatorios y su impacto en el sistema.

9. PRUEBAS DE INTEROPERABILIDAD Y SEGURIDAD

En base a la arquitectura presentada, se propone un conjunto de pruebas de interoperabilidad y seguridad con el fin de detectar vulnerabilidades, verificar el cumplimiento de estándares técnicos y validar los mecanismos de protección de datos para garantizar una implementación exitosa del sistema.

9.1. PRUEBAS DE CONECTIVIDAD Y COMUNICACIÓN

Con el objetivo de verificar la capacidad de la arquitectura para establecer conexiones seguras y confiables entre diferentes nodos e instituciones, se debe asegurar que los protocolos de comunicación, como MPGA, se implementen correctamente, y confirmar el uso de HTTP/2 y TLS 1.3 para garantizar la seguridad en la transmisión de datos.

Como criterios de aceptación se deben considerar que estas pruebas demuestren una latencia aceptable en el establecimiento de conexiones, el éxito en el intercambio de mensajes de prueba entre nodos y la verificación de la integridad de los mensajes mediante autenticación mutua y encriptación.

Algunas pruebas que podrían ser relevantes son:

1. **Pruebas de Conexión Persistente:** Dado que la conexión entre el nodo y el Módulo Central de PISEE 2.0 debe ser persistente, se pueden realizar pruebas para asegurar que la conexión se mantenga abierta. Esto implica verificar que tanto el nodo como el servidor pueda enviar y recibir información de manera continua (Guía Técnica de Interoperabilidad PISEE 2.0, p. 18).
2. **Pruebas de Seguridad de la Conexión:** La conexión debe utilizar TLS mutuo, lo que implica el intercambio de certificados para asegurar la autenticidad de las partes involucradas. Las pruebas deben verificar que los certificados se intercambian correctamente y que la conexión es segura (Guía Técnica de Interoperabilidad PISEE 2.0, p. 18).
3. **Pruebas de Service Discovery:** Dado que PISEE 2.0 ofrece un Service Discovery que contiene todas las URIs de los servicios, las pruebas deben asegurar que los nodos pueden acceder a este servicio y obtener la información necesaria para conectarse a otros servicios de la red (Guía Técnica de Interoperabilidad PISEE 2.0, p. 26).

9.2. PRUEBAS DE SEGURIDAD Y AUTENTICIDAD

Este tipo de testeos evalúan los mecanismos de seguridad implementados en la arquitectura para proteger la integridad y confidencialidad de los datos. Los objetivos son validar la autenticación mutua y el uso de tokens JWT para autorización, así como comprobar la encriptación de datos en tránsito y en reposo.

Los criterios de evaluación deben considerar la capacidad del sistema para rechazar accesos no autorizados, la eficiencia en la gestión de tokens y renovación de sesiones, y el registro y trazabilidad de eventos de seguridad.

Para evaluar la seguridad y autenticidad en la arquitectura propuesta, se pueden realizar las siguientes pruebas basadas en la información documentada:

1. **Prueba de Autenticación Mutua:** Verificar que el sistema realiza un intercambio y verificación de certificados de manera efectiva al abrir el canal de comunicación. Esto asegura que tanto el servidor como el nodo puedan identificar inequívocamente a su contraparte y confiar en ella. La autenticación se realiza mediante el uso de certificados obtenidos del Módulo de Certificados Públicos (Guía Técnica de Interoperabilidad PISEE 2.0, sección 7.1.1.c).

2. **Prueba de Autorización con Tokens JWT:** El sistema debe ser capaz de solicitar un token de autorización al Módulo Central de PISEE 2.0 y utilizarlo en los mensajes enviados al proveedor del servicio. Es crucial verificar que el token esté firmado digitalmente y que el proveedor del servicio pueda validar su firma y contenido (Guía Técnica de Interoperabilidad PISEE 2.0, sección 7.1.1.d).

3. **Prueba de Encriptación de Mensajes:** Comprobar que el sistema utiliza el protocolo TLS 1.3 para la encriptación de mensajes, asegurando que los datos en tránsito estén protegidos contra accesos no autorizados (Guía Técnica de Interoperabilidad PISEE 2.0, sección 7.1.1.e).

4. **Prueba de Rechazo de Accesos No Autorizados:** Evaluar la capacidad del sistema para rechazar accesos no autorizados, asegurando que solo los usuarios con los permisos adecuados puedan acceder a los servicios.

5. **Prueba de Gestión de Tokens y Renovación de Sesiones:** Verificar la eficiencia del sistema en la gestión de tokens, incluyendo la renovación de sesiones y la validez de los tokens durante el tiempo especificado.

6. **Prueba de Registro y Trazabilidad de Eventos de Seguridad:** Asegurar que el sistema registra metadatos asociados a cada transferencia de información en el Registro de Trazabilidad, utilizando un formato JSON estructurado, para garantizar la trazabilidad y validación de las operaciones realizadas (Guía Técnica de Interoperabilidad PISEE 2.0, sección 8).

7. **Pentesting periódico:** evaluar la seguridad del sistema en base a pruebas controladas de intrusión para detectar, analizar y documentar vulnerabilidades a fin de implementar medidas preventivas.

9.3. PRUEBAS DE RENDIMIENTO Y ESCALABILIDAD

Se debe evaluar la capacidad de la arquitectura para manejar cargas de trabajo variables y escalar según sea necesario con el objetivo de medir el rendimiento bajo diferentes niveles

de carga y asegurar que la arquitectura pueda escalar horizontalmente para agregar nuevas instituciones y servicios.

Para esto se deben estudiar y evaluar los tiempos de respuesta bajo condiciones de carga máxima y la capacidad para escalar sin comprometer el rendimiento. En esta línea, se propone:

1. **Pruebas de Escalabilidad:** Estas pruebas se enfocan en la capacidad del sistema para escalar horizontalmente. Se debe evaluar la facilidad con la que se pueden agregar nuevas fuentes de datos o servicios a la arquitectura, asegurando que el rendimiento no se vea afectado negativamente. Esto incluye la evaluación de la infraestructura tecnológica para integrar datos de múltiples fuentes institucionales bajo diversas modalidades, como se menciona en los términos de referencia del proyecto (Términos de Referencia para Consultoría de Interoperabilidad).

   Dentro de estas se recomiendan:

   Pruebas de Escalamiento Horizontal

   - Evaluación de auto-scaling en clusters de Kubernetes
   - Medición de latencia en balanceadores de carga
   - Pruebas de replicación de nodos
   - Verificación de consistencia en bases de datos distribuidas

   Integración de nuevas fuentes:

   - Testing de endpoints REST/SOAP
   - Validación de brokers de mensajería
   - Pruebas de transformación de datos (ETL)
   - Verificación de caché distribuido

2. **Pruebas de Carga:** Estas pruebas se centran en evaluar cómo la arquitectura maneja cargas de trabajo variables. Se debe medir el rendimiento bajo diferentes niveles de carga para asegurar que el sistema pueda manejar un aumento en el número de usuarios o transacciones sin degradar el rendimiento. Esto es crucial para verificar que la arquitectura puede escalar horizontalmente, permitiendo la adición de nuevas instituciones y servicios sin comprometer la eficiencia del sistema.

   Para esto se proponen:

   - Escenarios de Carga Progresiva
     - Benchmark con JMeter o K6 para simular según el número de usuarios concurrentes, transacciones por minuto, peaks de requests/ por hora y sostenibilidad de carga por 24 horas.

   - Monitoreo de Recursos
     - Medición de uso de CPU, memoria, network throughput, I/O operations y tiempo de respuesta.

   - Pruebas de Resiliencia
     - Conmutación por error (validación de cambio automático a sistemas de respaldo, verificación de continuidad de servicio, pruebas de redundancia de sistemas)
     - Validación de circuit breaker (pruebas de mecanismos de protección ante fallos, verificación de aislamiento de fallos, control de cascada de errores)
     - Tiempo de recuperación (tiempos de restauración de servicio y validación de procedimientos de recuperación)
     - Punto de recuperación (Verificación de respaldos y replicación y pruebas de consistencia de datos post-recuperación)

10. Estrategia de seguridad y protección de datos

La estrategia de protección y seguridad de los datos en el sistema de interoperabilidad ofrece un enfoque integral para enfrentar los desafíos propios de un entorno interinstitucional. Mediante la adopción de políticas claras y la coordinación continua entre los distintos actores, se promueve la integridad, confidencialidad y disponibilidad de la información, y se refuerza la confianza mutua. Este marco estratégico contempla la evolución técnica y organizativa, asegurando que las medidas de seguridad puedan adaptarse a nuevas exigencias normativas, al crecimiento del ecosistema y a las constantes transformaciones en el ámbito de la protección de datos.

10.1. Gobernanza de la Seguridad de la Información

La gobernanza define la estructura organizativa y los mecanismos necesarios para coordinar las decisiones relativas a la seguridad de la información. Estas recomendaciones buscan fortalecer la colaboración interinstitucional, asegurar la implementación de políticas homogéneas y gestionar eficientemente los riesgos.

- **Comité de Seguridad de la Información:** Crear un comité interinstitucional conformado por representantes clave de las entidades participantes. Este comité impulsará la creación e implementación de políticas de seguridad, la evaluación de riesgos emergentes y la propuesta de soluciones adaptativas. También tendría la responsabilidad de realizar revisiones periódicas con el fin de validar la eficacia de las medidas y su alineación con los estándares de interoperabilidad.

- **Responsable de la Estrategia de Datos:** Incorporar un rol dedicado al "negocio de los datos" permitirá establecer pautas claras sobre cómo procesar, gestionar y utilizar la información dentro del sistema. Este perfil definirá qué datos deben ser tratados, de qué manera se administran y con qué propósitos se emplean, manteniendo la alineación con los objetivos estratégicos de la solución. Asimismo, su participación será clave para garantizar el cumplimiento de las regulaciones vigentes y para generar valor a partir de los datos en el contexto de la interoperabilidad.

- **Oficial de Seguridad de la Información (OSI):** Se recomienda que cada OAE designe un OSI para supervisar localmente las labores relacionadas con la seguridad de la información. Esta figura actuaría como enlace con el Nodo Sectorial, promoviendo la adopción uniforme de políticas y asegurando una respuesta ágil ante incidentes. Además, el OSI lideraría iniciativas de capacitación, orientadas a que el personal conozca y aplique prácticas seguras de manejo de datos.

- **Equipo de trabajo especializado:** Se recomienda contar con un equipo especializado que incluya profesionales en redes con conocimiento en ciberseguridad, infraestructura de alta disponibilidad, arquitectura de software y metodologías ágiles (como Scrum). Este equipo trabajará en conjunto para diseñar, implementar y mantener las estrategias de seguridad necesarias, asegurando una integración técnica eficiente y adaptada a las necesidades del sistema. En casos donde sea factible, una misma persona podría asumir múltiples roles, como en redes e infraestructura que tenga capacidades de configuración de las reglas de firewall.

10.2. Gestión de Activos y Equipos

La adecuada gestión de los activos de información y de los equipos empleados en el sistema es esencial para prevenir brechas de seguridad. Estas recomendaciones permiten salvaguardar los recursos críticos y regular su acceso, atendiendo a las necesidades específicas de cada institución.

- **Gestión de Activos de la Información:** Se recomienda establecer un inventario completo y actualizado periódicamente de los activos de información críticos, clasificándolos de acuerdo con su nivel de sensibilidad y los riesgos asociados. Esta práctica posibilita focalizar los esfuerzos de protección, asignar responsables claros y aplicar controles específicos (por ejemplo, cifrado o restricciones de acceso) en función de la criticidad de cada activo.

- **Gestión de Equipos, Medios Móviles y BYOD:** Resulta fundamental regular el uso de dispositivos personales y móviles de quienes tengan permiso de administración en la plataforma mediante políticas claras, a fin de mitigar los riesgos inherentes al acceso remoto. Entre las medidas sugeridas destacan la configuración segura obligatoria, la adopción de cifrado de datos, la autenticación multifactor y la segmentación de la red para aislar los datos sensibles de los dispositivos personales.

10.3. Controles Técnicos y Operativos

Los controles técnicos resultan indispensables para proteger la infraestructura del sistema, mientras que los controles operativos garantizan la adecuada administración de datos y recursos. A continuación, se presentan acciones encaminadas a establecer medidas sólidas y escalables.

- **Control de Acceso:** Implementar un modelo de control de acceso basado en roles (RBAC) para delinear permisos específicos según las funciones de cada usuario. Este enfoque, combinado con la autenticación multifactor (MFA) y el monitoreo permanente, dificulta los accesos no autorizados.

- **Antivirus y Cortafuegos:** Desplegar soluciones de protección avanzadas en todos los puntos de acceso, especialmente Antivirus en los computadores de quienes tengan privilegios de administración y quienes tengan acceso a servidores. También se deben contar con servicios de antivirus en los servidores.

Los antivirus deben configurarse para ejecutar análisis periódicos y mantenerse actualizados, mientras que los cortafuegos han de filtrar el tráfico de manera efectiva, permitiendo solo las conexiones estrictamente necesarias.

- **Respaldo de Información:** Automatizar los respaldos periódicos de los datos críticos y almacenarlos en distintas ubicaciones geográficas contribuye a asegurar la disponibilidad frente a fallos o incidentes. Se recomienda cifrar dichos respaldos y efectuar simulacros periódicos para validar los tiempos de recuperación y la efectividad de los procedimientos. Debe quedar un registro de los respaldos junto con evidencia de las restauraciones. Considerar que los respaldos deben tener una caducidad y pasan a ser parte de los activos de información.

- **Registro y Seguimiento de Eventos:** Implementar un sistema de monitoreo que documente exhaustivamente todas las actividades en el entorno.Se debe Estos registros deben mantener un registro donde se indique qué dato fue entregado, por qué institución fue solicitado y compartido, y en qué fecha se realizaron estas acciones. Estos deben alojarse en repositorios seguros y conservarse durante los plazos establecidos por la normativa, facilitando las auditorías y la investigación forense de incidentes potenciales.

- **Administración de Licencias de Software:** Mantener políticas claras para la adquisición, registro y supervisión de licencias de software, tanto en servidores como en los equipos de administración de la plataforma, con el fin de reducir los riesgos asociados al uso de aplicaciones no autorizadas o desactualizadas. Asimismo, dichas políticas previenen vulnerabilidades de seguridad, garantizan el cumplimiento de la normativa de propiedad intelectual y disminuyen la probabilidad de incompatibilidades técnicas que afecten la estabilidad y el rendimiento del sistema..

- **Gestión de Vulnerabilidades Técnicas:** Llevar a cabo pruebas de penetración realizadas por un tercero, complementadas con escaneos automatizados continuos, para detectar vulnerabilidades antes de que sean explotadas. Asimismo, se recomienda acompañar estas acciones con un plan de priorización y aplicación de parches que aborde primero las brechas de mayor criticidad, reduciendo así el tiempo de exposición a riesgos.

- **Auditoría de Sistemas de Información:** La realización periódica de auditorías resulta clave para verificar la eficacia de los controles instalados. Estas evaluaciones abarcarían revisiones de configuraciones, políticas de acceso y cumplimiento normativo, asegurando la permanencia de altos niveles de seguridad en el sistema.

- **Gestión de Seguridad de las Redes:** Se recomienda segmentar la red a fin de limitar la propagación de ataques potenciales y contar con sistemas de detección y prevención de intrusiones (IDS/IPS) capaces de analizar el tráfico en tiempo real. Además, toda comunicación crítica debe protegerse mediante cifrado, reduciendo las probabilidades de interceptaciones.

10.4. Seguridad en el Desarrollo, Incidentes y Continuidad

La seguridad en el desarrollo de sistemas y la gestión de incidentes son pilares fundamentales para garantizar operaciones estables y confiables. Las siguientes recomendaciones buscan anticipar riesgos, permitir respuestas rápidas y salvaguardar la continuidad de las actividades esenciales.

- **Gestión de Cambios, Desarrollo y Pruebas:** Incorporar la seguridad en todas las fases de desarrollo bajo una perspectiva DevSecOps facilita la detección temprana de vulnerabilidades. Esto implica realizar revisiones automatizadas de código, verificar dependencias externas y aplicar controles de calidad exhaustivos en las pruebas.
- **Seguridad en el Desarrollo y Soporte:** Es recomendable restringir el acceso a los entornos de desarrollo y prohibir el uso de datos sensibles en las pruebas. Se sugiere, asimismo, definir controles para el soporte técnico (accesos autorizados, supervisión y registro de actividades) a fin de mantener la integridad y confidencialidad de la información.
- **Intercambio de Información (Convenios):** Los convenios interinstitucionales deben incluir disposiciones de seguridad específicas para el intercambio de datos, como el uso de cifrado (idealmente por PISEE 2.0), la definición de IP válidas para consulta de datos, la trazabilidad de las operaciones y la verificación de la integridad de la información. Estos acuerdos aportan claridad y garantizan que todas las partes cumplan con los mismos estándares de protección.
- **Seguridad de la Información Asociada a Proveedores:** Evaluar la idoneidad de los proveedores antes de contratarlos resulta esencial para confirmar que satisfacen los requisitos de seguridad deseados. Se recomienda asimismo contemplar auditorías periódicas en los contratos, asegurando que se mantengan altos niveles de protección durante todo el ciclo de vida de la relación comercial.
- **Gestión de Incidentes de Seguridad de la Información:** Contar con planes de respuesta bien definidos es clave para la detección, contención, análisis y notificación de incidentes. La práctica de simulacros regulares favorece la preparación organizacional y minimiza el impacto de los eventos de seguridad en la operación diaria. Esto cae dentro de la mejora continua en la que el análisis histórico de incidencias repetitivas permite corregir los problemas desde la causa.
- **Seguridad de la Información en Continuidad de Negocio:** Elaborar un plan de continuidad que considere redundancias en la infraestructura crítica, pruebas recurrentes de recuperación y políticas que mantengan las operaciones esenciales en escenarios de contingencia refuerza la resiliencia del sistema.

11. MECANISMOS DE CONTROL Y MONITOREO

A fin de mantener una visión integral del sistema interoperable y de fomentar su mejora continua, se proponen mecanismos de monitoreo y evaluación para asegurar el cumplimiento de los objetivos de la Ficha Única Laboral y Previsional.

11.1. MONITOREO TÉCNICO

Los mecanismos de monitoreo son importantes para asegurar la continuidad operativa, la seguridad, el rendimiento y la escalabilidad de la solución. Se establece un enfoque que abarca desde la recolección y visualización de métricas operativas hasta la gestión centralizada de logs y la trazabilidad de eventos. Este incluye:

1. **Monitoreo de servicios, balanceadores y nodos:** Para garantizar un monitoreo eficaz de la infraestructura, se establecerá un sistema de recolección de métricas que permita:
    - **Seguimiento del Rendimiento:** Captura en tiempo real de indicadores clave como el uso de CPU, memoria, latencia, tasa de errores y rendimiento de las conexiones.
    - **Visualización Centralizada:** Creación de dashboards personalizables que ofrezcan una visión global del estado de los componentes del sistema, facilitando la identificación de anomalías y tendencias en el comportamiento de la infraestructura.
    - **Alertas Basadas en Umbrales:** Configuración de alertas automáticas que se activen al superarse ciertos umbrales críticos, permitiendo una respuesta inmediata ante desviaciones o incidencias.
    - **Políticas de Auto-recuperación:** Configuración de reglas de reinicio automático y escalado dinámico, que aseguren la continuidad del servicio en caso de detectarse fallas o caídas en algún componente.
    - **Monitoreo del Cluster proveedor:** desempeño del balanceador de carga (distribución de tráfico y salud de nodos), los servidores APP en base a su rendimiento y disponibilidad, el caché centralizado según su *hit-ratio* y latencia, el rendimiento, replicación y consistencia de las bases de datos. Por último, la capacidad y latencia de acceso al sistema de archivos.

    - **Monitoreo del Cluster consumidor:** se deben supervisar la eficiencia en distribución del balanceador de carga, los tiempos de procesamiento de los nodos ETL, y la latencia del sistema de notificaciones.

    - **Monitoreo del Sistema pub/sub:** monitoreo de las actualizaciones de las fuente de datos compartidas en los canales de mensajería establecidos, el número de publicadores activos, la cantidad de suscriptores por tema, el volumen de mensajes por institución, los patrones de uso con sus peak de demanda, y la eficiencia en el enrutamiento de mensajes.

2. **Gestión Centralizada de Logs, Documentos y Auditorías de las peticiones:** La centralización y gestión eficiente de logs es esencial para la trazabilidad y auditoría de la operación del sistema. Para ello, se implementará un mecanismo que permita:

- **Consolidación de Registros:** Recopilación de logs provenientes de aplicaciones, ETL, servicios y nodos, centralizando la información para facilitar el análisis y la correlación de eventos.
- **Registro de Auditoría:** Conservación detallada de las acciones críticas y de acceso a la información, lo que facilita la verificación del cumplimiento normativo y la realización de auditorías internas y externas.

3. **Trazabilidad de Eventos y Transacciones:** Para comprender el flujo de datos y la ejecución de procesos dentro del sistema. Se implementará un mecanismo de trazabilidad distribuida que permita:
    - **Seguimiento de Transacciones:** Registro detallado de cada interacción o transacción a través de los distintos servicios y nodos, identificando el origen, destino, respuesta y el contexto de cada operación.
    - **Análisis de Flujo de Datos:** Mapeo completo del recorrido de la información, desde su origen hasta su consolidación en la Ficha Única, facilitando la identificación de cuellos de botella y la resolución de inconsistencias.
    - **Auditoría de Eventos:** Conservación del historial de eventos para facilitar investigaciones forenses y el análisis de incidentes, asegurando una respuesta oportuna ante cualquier anomalía detectada.
4. **Monitoreo de Seguridad y Cumplimiento Normativo:** Para proteger la integridad, confidencialidad y disponibilidad de la información. Se implementarán mecanismos para:
    - **Supervisión del Tráfico y Accesos:** Monitoreo continuo del tráfico de datos y las interacciones entre componentes, identificando patrones inusuales o accesos no autorizados.
    - **Detección de Vulnerabilidades:** Integración de procesos de análisis continuo que permitan identificar vulnerabilidades en el código y en la configuración de la infraestructura, facilitando su pronta remediación.
    - **Registro y Auditoría de Seguridad:** Mantenimiento de registros detallados de todas las acciones relacionadas con la seguridad, lo que permitirá verificar el cumplimiento de políticas y normativas de protección de datos.
5. **Centralización y Visualización Integral:** Para facilitar la gestión y el análisis de los diferentes mecanismos de monitoreo, se implementará una **plataforma de administración** que centraliza la información proveniente de las distintas fuentes. Esta solución deberá:
    - **Integrar Métricas, Logs y Trazabilidad:** Consolidar la información operativa en una única interfaz, permitiendo a los equipos de soporte acceder a datos detallados y correlacionados de manera rápida y eficiente.
    - **Ofrecer Visualizaciones:** Permitir la visualización de dashboards adaptados a las necesidades de distintos roles, desde administradores de sistemas hasta equipos de auditoría y seguridad.
    - **Facilitar la Toma de Decisiones:** Proporcionar informes y análisis en tiempo real que apoyen la toma de decisiones estratégicas y operativas, optimizando la respuesta ante incidentes y la planificación de recursos.

11.2. MODELO DE GOBERNANZA DE DATOS

Establece el marco que rige las políticas, procesos y responsabilidades para el control, la administración y la protección segura de los datos intercambiados en el sistema interoperable. Se definen roles, normativas, mecanismos de control y propuestas innovadoras para garantizar la integridad, confidencialidad, disponibilidad y uso adecuado de la información.

11.2.1. Estructura organizacional

Dentro de los roles claves en términos de gobernanza para la implementación del sistema, además de los ya mencionados en el capítulo 10.1, se encuentran:

- **Administrador de Datos (Data Steward):** Es responsable de asegurar la calidad, la integridad y la seguridad de los datos dentro del sistema interoperable. Este rol implica definir políticas de acceso a los datos, clasificar los datos según su sensibilidad y asegurar que se cumplan las normativas de protección de datos, como la Ley de Datos Personales (N° 21.729). Además, debe coordinar la implementación de procesos de validación y depuración de datos.

- **Oficial de Gobernanza de Datos (Data Governance Officer):** Supervisa el cumplimiento de las políticas de gobernanza de datos y privacidad en cada organización involucrada. Aunque no se involucra directamente en la implementación técnica, este rol debe asegurar que el sistema opere dentro del marco legal y normativo aplicable, así como para gestionar los riesgos relacionados con los datos. El oficial de gobernanza de datos debe promover la formación y actualización continua de temas de protección y administración de datos.

- **Comité Interinstitucional de Gobernanza de Datos:** Un organismo colaborativo que reúna representantes de todas las OAEs involucradas. Este comité tiene como objetivos definir lineamientos comunes para la gestión y el intercambio de datos; Resolver discrepancias y promover la estandarización de prácticas; Evaluar periódicamente la efectividad de las políticas implementadas y proponer mejoras.

11.2.2. Políticas y Normativas

El modelo de gobernanza se sustenta en un marco normativo robusto, que asegure la operación segura del sistema y el cumplimiento legal. Entre las normativas y políticas clave se encuentran:

- **Ley de Protección de Datos Personales:** esta normativa promulgada en 2024 establece un marco para el tratamiento de información personal, exigiendo medidas específicas para garantizar la privacidad y seguridad de los datos de los ciudadanos. Esta ley requiere implementar controles estrictos sobre el acceso, procesamiento y almacenamiento de datos personales, además de establecer responsabilidades claras para su gestión.

- **Acuerdos de Nivel de Servicio (SLAs):** se recomienda adoptar un acuerdo global (sectorial) que involucre a todas las OAEs relevantes para la Ficha Única. En este se

deben definir métricas específicas y medibles para asegurar la calidad del servicio interoperable, estableciendo claramente los niveles de disponibilidad, tiempos de respuesta y procedimientos de resolución de incidentes para cada OAE, proporcionando un marco de referencia para evaluar y mantener la calidad del servicio.

- **Estándares técnicos de PISEE 2.0:** se debe seguir el marco de referencia dispuesto para la interoperabilidad entre OAEs. Estos estándares aseguran la compatibilidad y eficiencia en el intercambio de información, estableciendo protocolos y formatos específicos para la comunicación entre sistemas.

- **Decreto 83:** establece cuatro atributos esenciales para la seguridad de documentos electrónicos: **confidencialidad para proteger la información sensible, integridad para garantizar que los datos no sean alterados, factibilidad de autenticación para verificar la identidad de los participantes, y disponibilidad para asegurar el acceso continuo a los servicios**. Estos atributos deben implementarse mediante controles técnicos y procedimientos específicos que aseguren su cumplimiento efectivo dentro del sistema interoperable.

11.2.3. Mecanismos de Control y Cumplimiento

El marco de control y cumplimiento se basa en tres pilares que guían la gestión y protección de los datos institucionales, necesarios para proteger los datos, asegurar su uso adecuado y mantener la confianza en el sistema interoperable.

- **Principio de Finalidad:** Los datos deben ser accesibles solo con un fin específico y restringidos según el propósito de cada procedimiento administrativo. Esto asegura que el acceso a los datos esté alineado con los objetivos específicos de cada proceso.

- **Clasificación y Protección de Datos Sensibles:** Es crucial identificar los datos que requieren protección especial y establecer mecanismos para limitar el acceso y asegurar su encriptación si es necesario a fin de proteger la información sensible de accesos no autorizados. Se deben implementar mecanismos que limiten el acceso a datos sensibles y asegurar su encriptación durante el almacenamiento y transmisión.

- **Responsabilidad y Validación en las OAEs:** Cada OAE involucrada en el proyecto debe aplicar validaciones para garantizar la correcta interpretación de los datos, asegurando que estos sean utilizados de manera precisa y adecuada. Esto incluye auditorías periódicas y revisiones de procesos, garantizando que cada institución cumpla con las políticas establecidas. Además, la gobernanza se refuerza mediante acuerdos claros sobre la asignación de responsabilidades respecto a las fuentes de datos, promoviendo la colaboración y el intercambio seguro de información.

11.2.4. Propuestas Adicionales para el Fortalecimiento de la Gobernanza de Datos

Para robustecer la gobernanza de datos se proponen iniciativas orientadas a elevar la calidad y la seguridad en el manejo de la información. En primer lugar, es fundamental implementar un **marco de calidad de datos** que establezca indicadores y métricas para evaluar la

precisión, consistencia, integridad y actualidad de la información. Este enfoque permitirá realizar auditorías periódicas que identifiquen discrepancias y aseguren que los datos sean confiables y se alineen con los objetivos de cada procedimiento administrativo.

Se sugiere el desarrollo de un **portal de transparencia y reportes**, el cual centralice la visualización de indicadores clave y ofrezca acceso en tiempo real a información relevante sobre el desempeño del sistema. Esta plataforma facilitará la rendición de cuentas y respalda la toma de decisiones mediante informes detallados que muestren la evolución y calidad de los datos.

Es clave **fomentar una cultura de datos** sólida a través de programas de capacitación y formación continua para todos los actores involucrados. La difusión de buenas prácticas y el desarrollo de competencias en el manejo seguro de la información contribuirán a que cada institución adopte procedimientos adecuados y se comprometa con la protección de los datos.

Finalmente, se plantea la **integración de herramientas de monitoreo y auditoría** que permitan un seguimiento constante del flujo de información y la detección temprana de incidencias. Estas soluciones automatizadas facilitarán la generación de informes y alertas, garantizando respuestas oportunas ante cualquier desviación o anomalía.

12. Plan de implementación

12.1. Metodologías de trabajo

Se propone la implementación de metodologías ágiles que permitan optimizar tanto el desarrollo como la operación continua del sistema. Durante la fase de desarrollo e integración se implementará SCRUM proporcionando un marco de trabajo iterativo e incremental que facilitará la construcción progresiva de las capacidades de interoperabilidad esperadas, con validación temprana las integraciones y adaptación a cambios en especificaciones técnicas. Esta se ejecuta a través de ciclos de desarrollo cortos (sprints, de dos a cuatro semanas) donde los equipos podrán entregar funcionalidades incrementales y validar su efectividad de manera continua.

12.2. Planificación

12.2.1. Fase 1: Preparación e Implementación (6 meses) - inicio mayo 2025

Establecer las bases legales, organizativas y tecnológicas que permitan la interoperabilidad entre las distintas instituciones, culminando con una primera puesta en marcha controlada (Marcha Blanca), enfocándose en los siguientes elementos:

1. **Revisión de Lineamientos y Convenios**

   Como se comentó en el capítulo de *Convenios entre OAEs*, para abordar esta solución de la Ficha Única, a través del nodo sectorial, se deben formalizar acuerdos legales que permitan la consolidación de la información de una forma ágil. Estos acuerdos deben abrir las puertas a nuevas instituciones para que el sistema sea flexible en el escalamiento de los consumidores/proveedores.

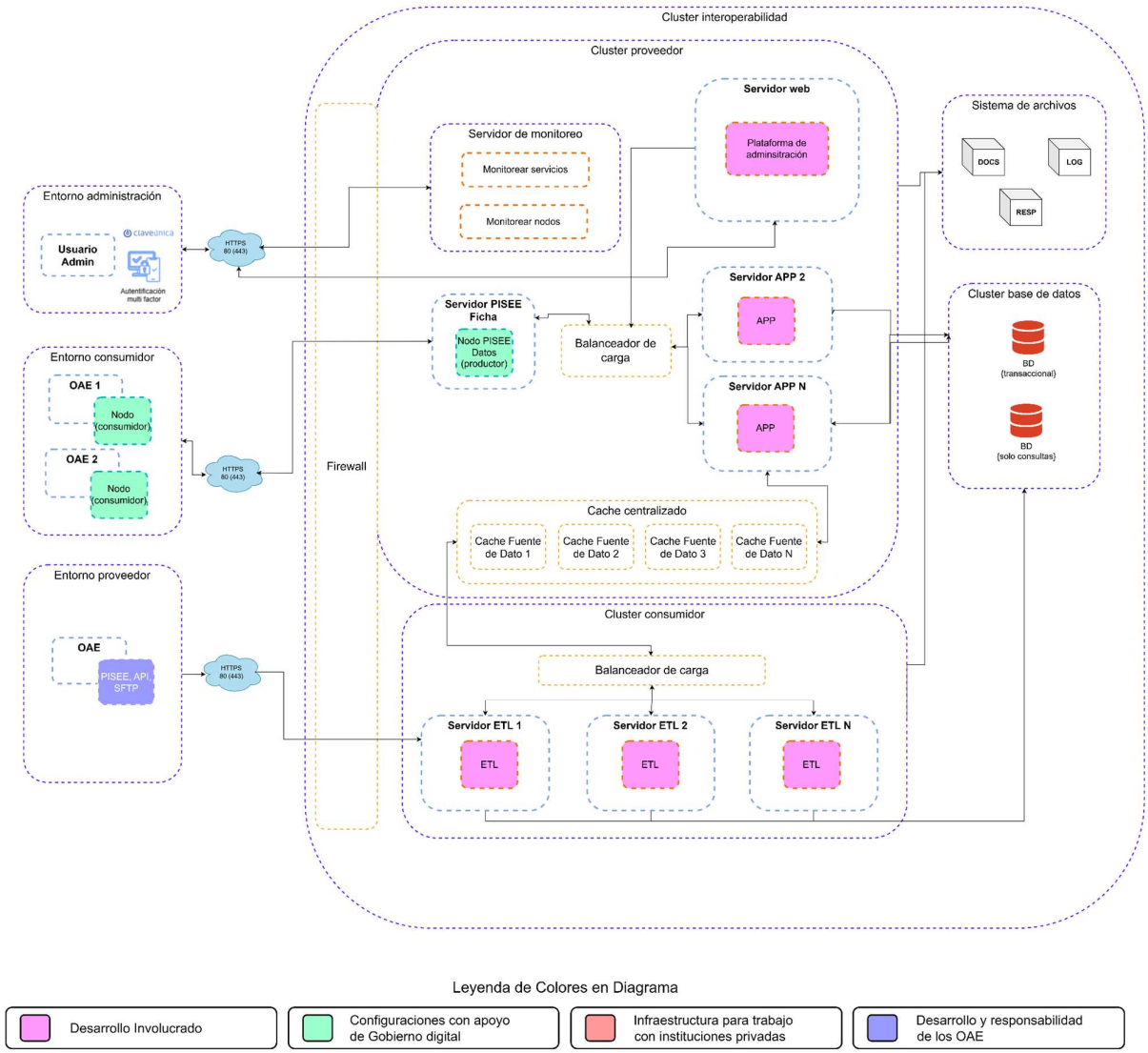
2. **Roles y Gobernanza**

   Por otro lado, se deben establecer responsabilidades específicas para cada OAE. Esto considera tanto en términos de *Gobernanza*, como de los roles de *Seguridad del Dato* que se abordan en la seguridad de los datos. Este proceso incluye la validación de los aspectos regulatorios, con la participación de asesoría jurídica, y el establecimiento de criterios claros para el intercambio de datos, asegurando así el cumplimiento de la normativa vigente.

3. **Implementación Técnica y Pruebas**

Inicialmente, la infraestructura a implementar se enfocará en la construcción del funcionamiento base del nodo sectorial y la consolidación de la información de un grupo inicial de OAEs. Es decir, se implementa gran parte del Cluster de Interoperabilidad. Esto incluye:

- La implementación del *Cluster Proveedor*
    - Conectando el nodo sectorial a las OAEs como únicas consumidoras del servicio.
    - Habilitando completamente los servidores que permiten la escalabilidad del sistema.
    - El *Caché Centralizado* que permita almacenar temporalmente por separadas las fuentes de datos que entrega a pedido el cluster consumidor.
- Un *Sistema de Archivos* que almacene documentos, logs y respaldos de las transacciones en el sistema con un fin auditable desde la implementación.
- El *Cluster Base de Datos* que permite almacenar data transaccional, un catálogo de eventos y data que requiera almacenaje para la recepción, como fuentes de datos transferida por masiva
- Por último, el *Cluster Consumidor* con un balanceador de carga conectado a los servidores que solicitan la data demandada por el *Cluster Proveedor* y permiten filtrar el contenido solicitado (no modificar el dato específicamente).



Leyenda de Colores en Diagrama

Desarrollo Involucrado	Configuraciones con apoyo de Gobierno digital	Infraestructura para trabajo con instituciones privadas	Desarrollo y responsabilidad de los OAE

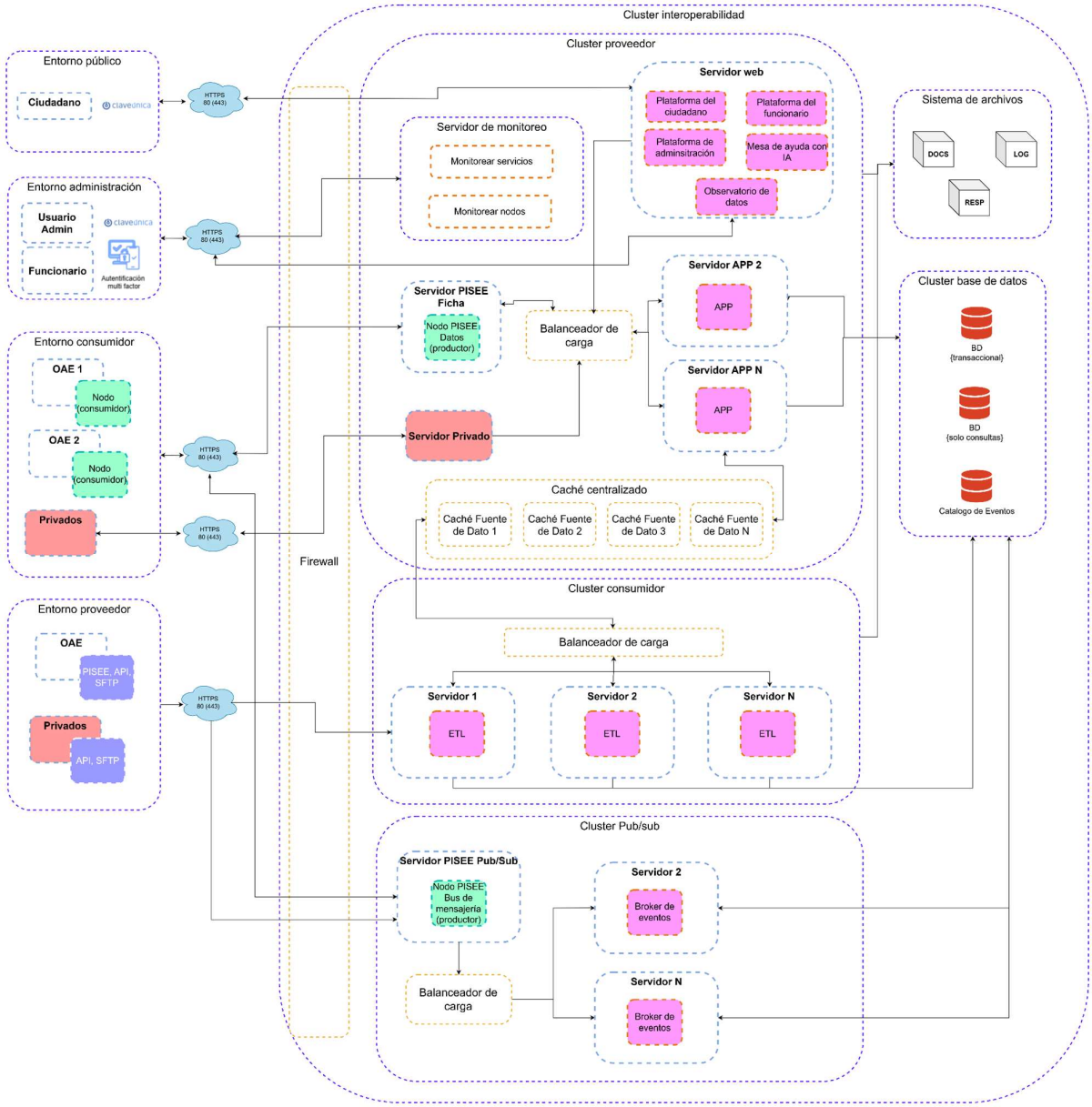
Una vez implementado lo anterior, se procede a realizar pruebas de conectividad, comunicación y rendimiento en ambientes de QA y preproducción, afinando la configuración hasta lograr la estabilidad requerida. El enfoque es garantizar que el sistema cumpla con los requisitos funcionales y de seguridad antes de avanzar a la producción.

4. **Marcha Blanca con Grupo Pionero**

   Finalmente, se despliega la plataforma en producción de manera controlada con un primer grupo de instituciones que presentan mayor madurez y demanda de datos. Durante esta Marcha Blanca, se supervisa de forma constante la respuesta del sistema bajo condiciones cercanas a la operación real. Los ajustes finales de rendimiento y seguridad se abordan en función de los resultados obtenidos, sentando las bases para una adopción más amplia en fases posteriores.

12.2.2. Fase 2: Expansión y mantenimiento evolutivo (hasta diciembre 2026)

Esta segunda etapa se enfoca en ampliar la capacidad transaccional del sistema, desarrollar nuevas funcionalidades y asegurar la continuidad operativa mediante el monitoreo constante de las instituciones ya integradas.



1. **Expansión de Infraestructura:**
    - Establecer la conexión entre la Plataforma Web y el nodo sectorial, incorporando la autenticación con ClaveÚnica de ciudadanos y de funcionarios (sumado MFA).
    - Implementación de Observatorio de Datos
    - Incorporación de sistema Pub/Sub, que permite realizar la reportería sobre la actualización de la información de las OAEs de interés para consumidores del sistema.
    - Implementación de asistencia AI, representado por un Chatbot con AI en la plataforma.

2. **Mantención Evolutiva**
    - Incorporación de nuevas fuentes de datos por OAEs participantes
    - Incorporación Progresiva de Instituciones (Grupo 2) - Últimos 6 meses 2026
        i. Capacitación y acompañamiento: Formar a las instituciones de madurez media en el uso y la gestión del sistema de interoperabilidad.
        ii. Extender la infraestructura para admitir un mayor número de conexiones y nodos.
        iii. Integración gradual: Supervisar la adopción y el rendimiento de cada institución, ajustando los recursos según sea necesario.

3. **Monitoreo de Grupo 1**
    - Aplicar la estrategia de pruebas establecida para confirmar que el sistema mantiene niveles adecuados de rendimiento bajo distintas cargas.
    - Registrar métricas e indicadores clave (tiempos de respuesta, uso de CPU, memoria, etc.) para reaccionar oportunamente ante posibles incidencias.
    - Resolver oportunamente incidencias para mantener la operatividad del sistema.

4. **Mantención y Soporte**
    - Corrección de bugs
    - Optimizaciones de rendimiento
    - Peticiones realizadas por institución (analizarlo por horarios del día, días de semana, días del mes, etc.)
    - Implementación de nuevos mecanismos de Ciberseguridad

5. **Monitoreo de métricas de:**
    - Eficiencia/desempeño (tiempos de respuesta por institución)
    - Revisión de licencias y métricas de seguridad
    - Cual es el uso de recursos de los servidores (no debe superar el 80% del uso de recursos)
    - Monitoreo de espacio de disco (Logs, Caché, etc.)

12.3. Gestión y Coordinación del proyecto

La implementación del proyecto requiere una articulación efectiva entre el Ministerio del Trabajo y Previsión Social, la Subsecretaría de Previsión Social (SPS), la Secretaría de Gobierno Digital (SGD) y los Organismos Autónomos del Estado (OAEs). Cada actor cumple un rol específico y su coordinación es fundamental para garantizar la interoperabilidad, la seguridad de la información y la eficiencia operativa.

- **Ministerio del Trabajo y Previsión Social:** Supervisa el avance estratégico del proyecto, asegurando que se cumplan los objetivos de modernización e interoperabilidad del sector y actuando como enlace clave entre las diversas entidades gubernamentales para garantizar apoyo institucional y sostenibilidad a largo plazo.
- **Subsecretaría de Previsión Social (SPS):** Es el principal impulsor del proyecto y responsable de su ejecución operativa; coordina con las OAEs para integrar datos en la Ficha Única, define los estándares de interoperabilidad y la estructuración de la información. Con el fin de sustentar lo anterior:
    - Este actor es quien debiera llevar desde un inicio el modelo de gobernanza establecido en la sección 11.2. Modelo de Gobernanza.
    - Gestionar el equipo técnico encargado de la implementación.
    - Organiza comités periódicos para evaluar avances y resolver desafíos técnicos y operativos, levantados por los distintos actores del estado.
- **Subsecretaría de Gobierno Digital (SGD):** Provee la plataforma PISEE 2.0, fundamental para la interoperabilidad y comunicación entre nodos, guía la adopción de estándares tecnológicos para que los participantes logren conectarse al sistema interoperabilidad de datos, supervisando junto a SPS la implementación de medidas de seguridad y gobernanza digital para garantizar el cumplimiento normativo.

  Al ser el administrador y gestor del sistema PISEE, este participante es quien crea y mantiene los “puentes” que unen las “islas” dentro del sistema interoperable, permitiendo una conexión cifrada y segura.

- **Organismos de la Administración del Estado (OAEs):** Actúan como los principales proveedores y consumidores de datos; deben asegurar que sus sistemas internos sean compatibles con el sistema PISEE y la demanda estimada de sus servicios. Dentro de las principales funciones se encuentran

    - Apoyar en el establecimiento de acuerdos entre sus proveedores/consumidores (otras OAEs), para lograr la centralización de las fuentes de datos sectoriales.

    - A partir de lo anterior, definir las alertas y fuentes de interés del organismo en el sistema para participar activamente en el modelo de Publicación/Suscripción (Pub/Sub) para el intercambio automático y en tiempo real de información.

    - Guiarse por el modelo de gobernanza establecido en la sección 10.1. Gobernanza de la Seguridad de la Información.

Lo anterior debe ser sustentado por un convenio sectorial integral que unifique las condiciones para el acceso, uso y protección de los datos, como el que se establece en la sección "6.2. Convenios OAEs". Este acuerdo, de alcance general, permitiría que el nodo sectorial asuma de forma centralizada la gestión operativa y técnica de las transacciones, estableciendo controles de acceso basados en roles y garantizando la trazabilidad completa de cada operación para cumplir con las normativas vigentes.

Finalmente, la implementación de este sistema, guiada por la estrategia anterior, permitiría mejorar los procesos actuales empleados por cada organismo del estado y adherirse al cumplimiento de la normativa de transformación digital. Principalmente:

- Al centralizar el intercambio de datos y automatizar procesos, se reducen las tareas manuales y se acortan los tiempos de respuesta, permitiendo un funcionamiento más ágil de los trámites.

- Con mecanismos centralizados de control de acceso y protocolos de encriptación, se protege la confidencialidad y la integridad de los datos, reduciendo el riesgo de ciberataques y garantizando el cumplimiento de normativas de protección de datos.

- La arquitectura del sistema permite la incorporación gradual de nuevas instituciones y fuentes de datos sin comprometer la estabilidad, lo que asegura que la solución pueda evolucionar y adaptarse a futuros requerimientos.

- Gracias a la flexibilidad del sistema para aceptar diversos mecanismos de transferencia de datos (como WS, API y SFTP), incluso los organismos con menores capacidades tecnológicas pueden integrarse de forma sencilla. El sistema se encarga de procesar y normalizar los datos que se le entregan, evitando que la nueva OAE tenga que desarrollar procesos adicionales.

  Por el lado de un nuevo consumidor del sistema, al consolidar toda la información de los participantes en una ficha unificada en formato JSON, los nuevos organismos no necesitan modificar sus endpoints (Nodo PISEE como canal constante de solicitud), ni ajustar drásticamente sus procesos de ETL cada vez que se añade una nueva fuente de datos a la solicitud.

ANEXOS

ANEXO 1: INTERCAMBIO DE INFORMACIÓN/FUENTES DE DATOS

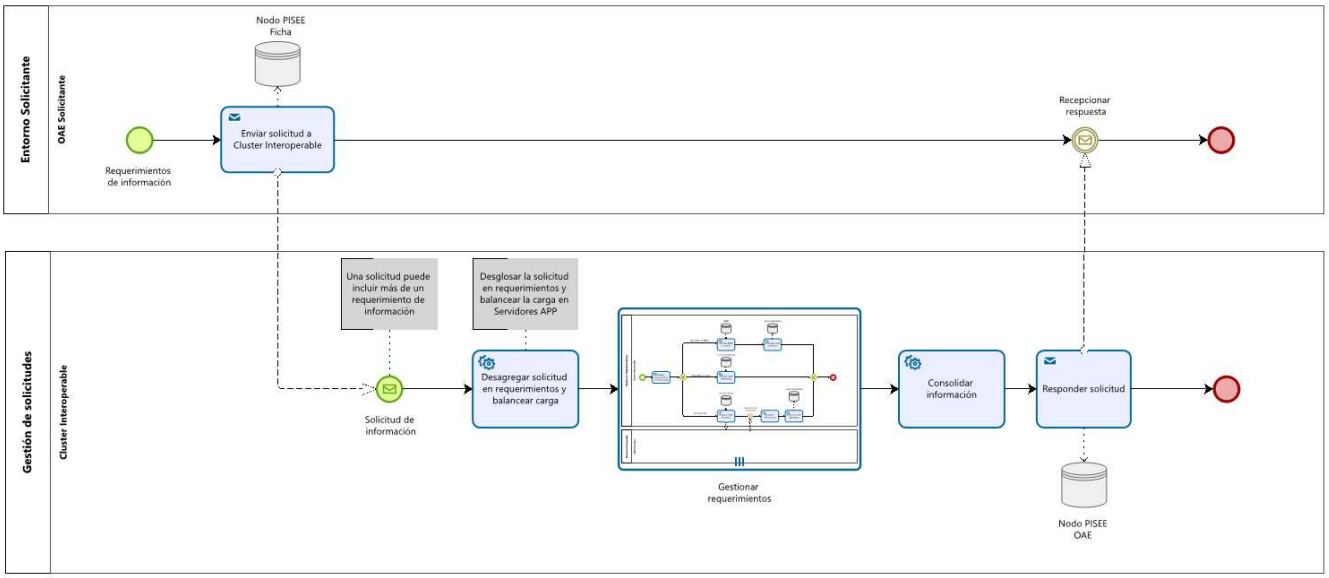
Como se mencionó anteriormente, uno de los elementos clave de la solución a diseñar son las OAEs, cuyo propósito es garantizar la capacidad del sistema, su infraestructura y las conexiones necesarias en el ecosistema de interoperabilidad. Para avanzar en este objetivo, se está trabajando con una matriz de oferta y demanda de los servicios que las instituciones habilitan, tanto a través de PISEE como por otros medios de transferencia. De manera complementaria, se analizan los registros de interoperabilidad del CPAT para ajustar esta matriz y obtener una visión clara del contexto actual que se busca perfeccionar.

ANEXO 2: DIAGRAMA OPERATIVO DEL SISTEMA

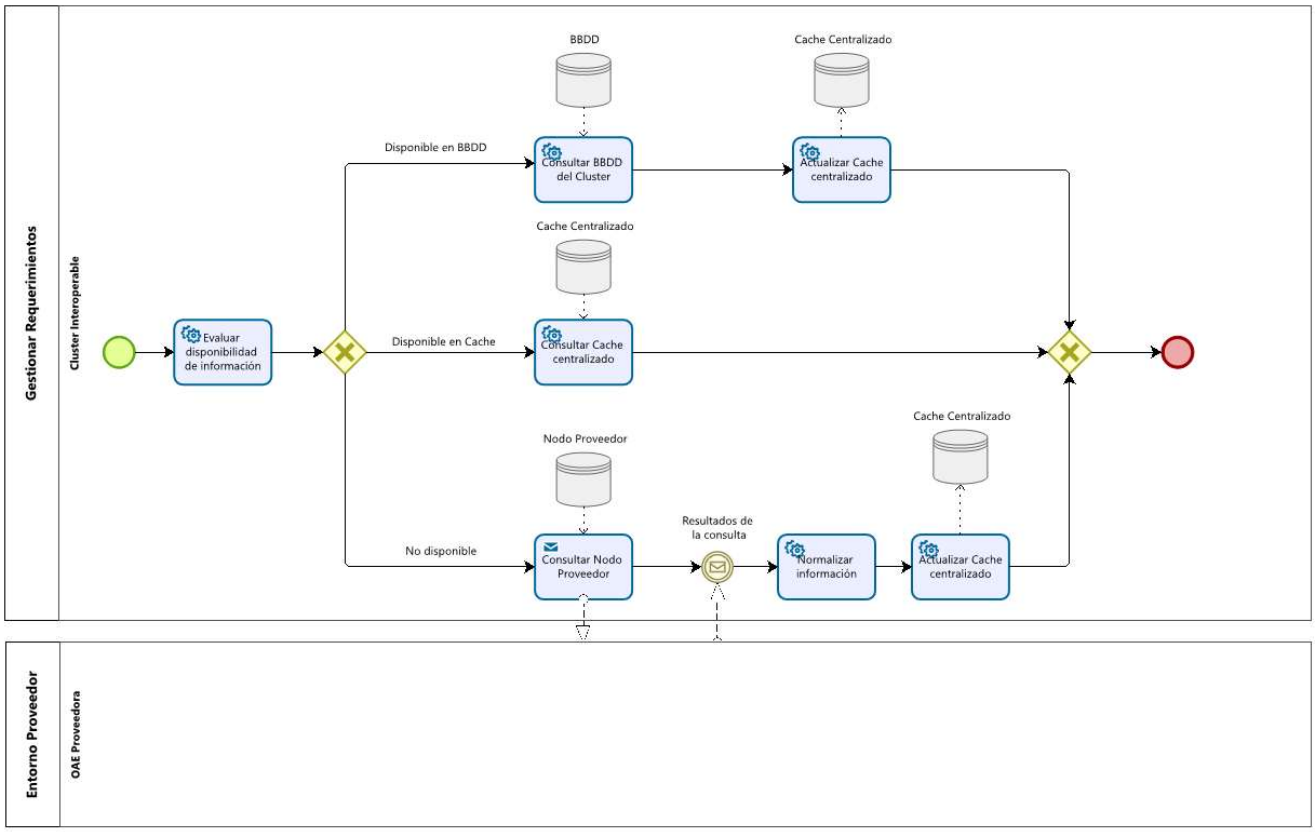
En este anexo se entregan BPMNs que ilustran algunos casos de uso diseñados para comprender el proceso asociado a la solicitud de fuentes de datos. Específicamente cómo las OAEs y el entorno público pueden realizar esta petición a través del cluster de interoperabilidad, el cual consolida y entrega la información en la Ficha Única apoyándose del entorno proveedor.

ANEXO 2.1. CASO "OAE SOLICITA FUENTES DE DATOS"

En el caso que una OAE quiera realizar una solicitud de datos al sistema interoperable, ésta se comunica a través del Nodo PISEE Ficha o Sectorial, que actúa como puerta de entrada al cluster de interoperabilidad. Una vez que la petición llega, el balanceador de carga distribuye la solicitud a los servidores APP del entorno Proveedor.

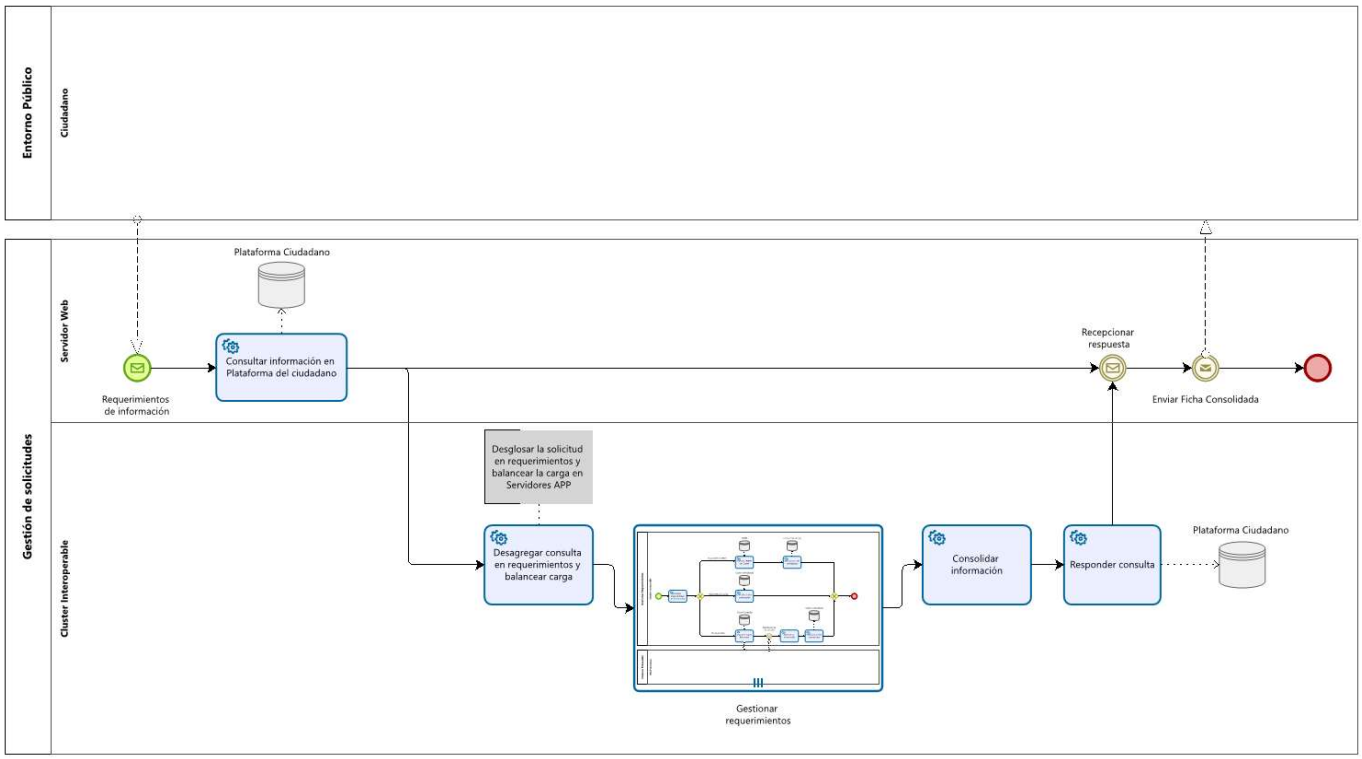


Aquí, cada fuente de datos solicitada entra en el subproceso de gestión de requerimientos y evalúa de forma inmediata si la respuesta se encuentra en el caché centralizado. Si es así, se retorna la fuente de datos almacenada, sin necesidad de realizar más procesos. Si no se encuentra en el caché, el servidor APP decide cuál de las otras dos rutas seguir: si la solicitud corresponde a un archivo de carga masiva (como en el caso de las fuentes de datos de la Dirección del Trabajo), se consulta la base de datos "consultas"; si se trata de datos transaccionales (accesibles mediante Web Service o API), se envía la solicitud al cluster Consumidor, donde los servidores ETL se encargan de extraer, transformar y normalizar la información proveniente de las OAEs proveedoras, generando un JSON consolidado que se integra y se devuelve como parte de la Ficha única.


Gestionar Requerimientos
Cluster Interoperable
BBDD
Cache Centralizado
Disponible en BBDD
Consultar BBDD del Cluster
Actualizar Cache centralizado
Cache Centralizado
Evaluar disponibilidad de información
Disponible en Cache
Consultar Cache centralizado
Cache Centralizado
Nodo Proveedor
No disponible
Consultar Nodo Proveedor
Resultados de la consulta
Normalizar información
Actualizar Cache centralizado
Entorno Proveedor
OAE Proveedora

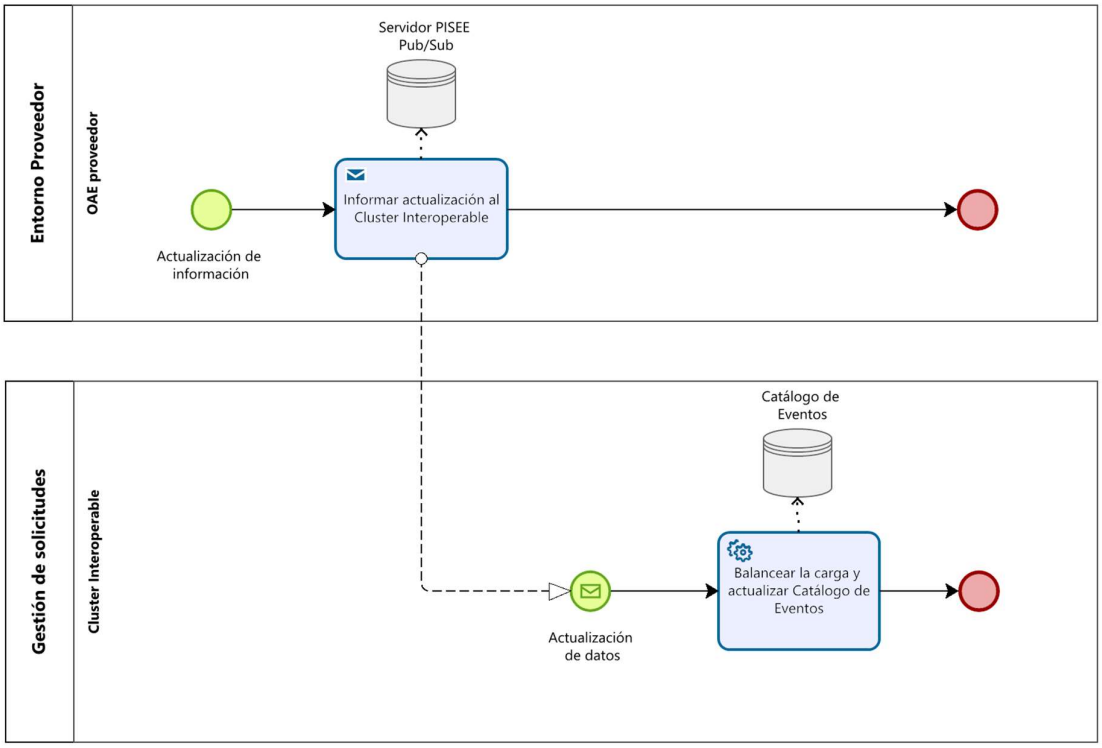
ANEXO 2.2. CASO "CIUDADANO SOLICITA SU FICHA ÚNICA"

En el caso de un ciudadano que solicita la Ficha Única, el proceso se inicia desde la plataforma web, luego de autenticarse con clave única. Aunque la interfaz para realizar la petición es más sencilla, el proceso para realizar la solicitud de las fuentes de datos es similar: la petición llega al cluster de interoperabilidad, donde el balanceador distribuye la solicitud a los servidores APP, que inmediatamente verifican si la información ya está en el caché. De no estarlo, el sistema determina si debe consultar la base de datos "consultas" (en caso de datos de carga masiva) o bien remitir la solicitud a los servidores ETL para procesar datos transaccionales, y así conformar la Ficha única presentada al ciudadano.

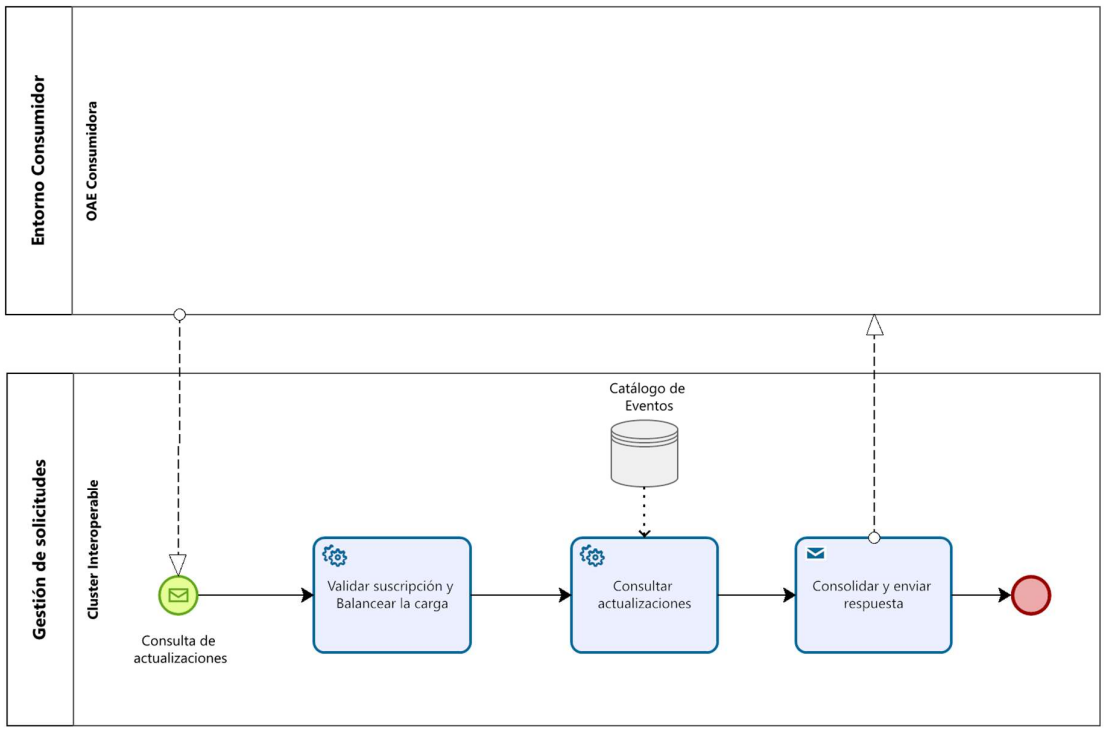


ANEXO 2.3. CASO "PUB/SUB"

Finalmente, en el mecanismo Pub/Sub, cuando una OAE proveedora actualiza sus datos, la notificación se envía a través del Nodo PISEE Pub/Sub. El balanceador dirige la actualización a los brokers de eventos, y esta se registra en el catálogo de eventos.



Por otro lado, las OAEs suscriptoras/consumidoras reciben la notificación a través del mismo Nodo PISEE Pub/Sub y, en función de esta, pueden activar el mismo proceso de solicitud a la fuente de datos para acceder a la información actualizada.



ANEXO 3 TEMPLATE DE LEVANTAMIENTO

Paralelamente, a través de sesiones con las OAEs, se recopilan datos sobre los procesos que cada institución utiliza para intercambiar información, los medios empleados (incluido PISEE), la infraestructura que sostiene dichos intercambios y las necesidades que podrían surgir ante la implementación de la nueva solución. Toda esta información se integrará en un template de levantamiento, estructurado en cuatro secciones principales, a fin de facilitar la organización y visibilización de cada aspecto esencial para la ejecución exitosa de la propuesta.

Sección 1 - Información General de la OAE

Identificación de la OAE

Nombre de la institución.	
Código único de identificación (si aplica).	

Contraparte Institucional

Responsable de transformación digital (nombre + mail)	
Encargado de informática (nombre + mail)	

Sección II - Descripción del Intercambio de Datos

Fuente de datos		Propósito del Intercambio de Datos:		
Nombre de fuente de datos	Responsable del intercambio (nombre, cargo, contacto).	Objetivo general.	Relación con procesos o trámites administrativos.	Con quienes tienen convenio de intercambio de datos (OAE)

Origen del dato	Descripción del Mecanismo de Transferencia:			
La data proviene de algún web service, de alguna institución o se genera en esta institución?	Tipo: Web Service (WS), Archivo Plano, PISEE 1.0/2.0.	Justificación de selección del mecanismo.	Mecanismo de autentificación	Mecanismo de seguridad adicional si existe

Con la información que se recopila a través de las reuniones y los antecedentes entregados como la matriz y el registro CPAT, se rellena esta sección para cada servicio o fuente de datos. Cuando se habla de *fuente de dato*, se hace alusión a la información/data que está disponible para envío entre instituciones, por ejemplo, beneficios activos de un ciudadano, situación laboral, etc.

Sección III - Información de Datos a Transferir

Fuente de dato	Tipos de datos a compartir (planillas, data transaccional, archivos, etc)	Periodicidad del intercambio (real-time, batch).	Volumen estimado (número de registros, peso en Gb).	Crecimiento mensual de la fuente de datos (número de registros, peso en Gb)	Reglas de consistencia y validación (codificación, validación de columnas, entre otros)	Tolerancia a errores.	¿Existe un diccionario de datos? (Si/No)	Adjuntar muestra de datos	Comentarios adicionales
1									
2									
3									
4									
5									
...									

Por otro lado, se analiza la demanda que tienen las fuentes de datos ofertadas por la institución, permitiendo conocer la capacidad necesaria desde la OAE que requerirá en un futuro, considerando el crecimiento de solicitudes, dando claridad del escalamiento que estas requerirán.

Sección IV - Información Demandada

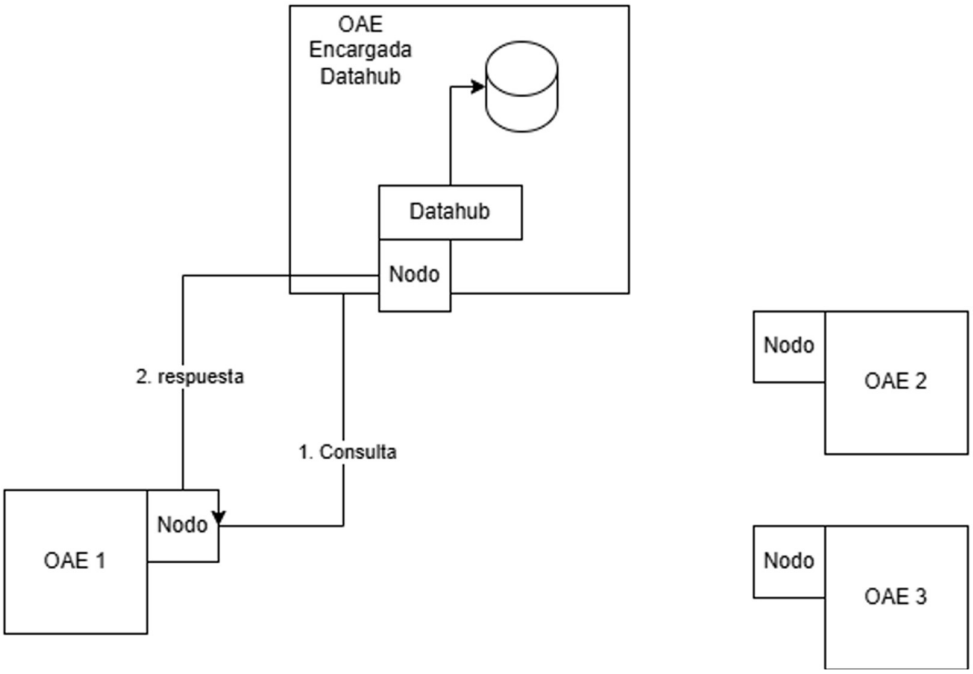
Fuente de dato	Tipos de datos a compartir (planillas, data transaccional, archivos, etc)	Institución u organismo del cual se solicita la información	Campos solicitados (variables en particular)	Procedimiento administrativo	Frecuencia con la que se necesita la actualización del dato	Propósito o uso esperado	Impacto de la no disponibilidad (impacto operativo en caso de no disponer)	Responsable del requerimiento (quien emite la solicitud del requerimiento)	Comentarios adicionales
1									
2									
3									
4									
5									
...									

Por último, se busca conocer cuáles son las fuentes de datos que consume la OAE para hacer contraste con la oferta de las otras involucradas y entender el nivel de demanda que se tiene y se tendrá en la nueva solución.

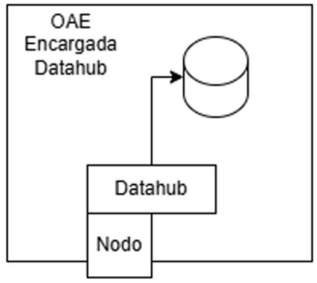
ANEXO 4: ESQUEMAS TÉCNICOS DE INTEROPERABILIDAD

Previo a al diseño de la arquitectura inicial, se realizó una iteración de lo que se esperara fuera el sistema de interoperabilidad que permitiera sustentar la Ficha Única laboral y previsional. A continuación, se muestran los esquemas técnicos propuestos para el sistema de interoperabilidad, basados en escenarios de consulta (una OAE solicitando información que puede proporcionar otra OAE).

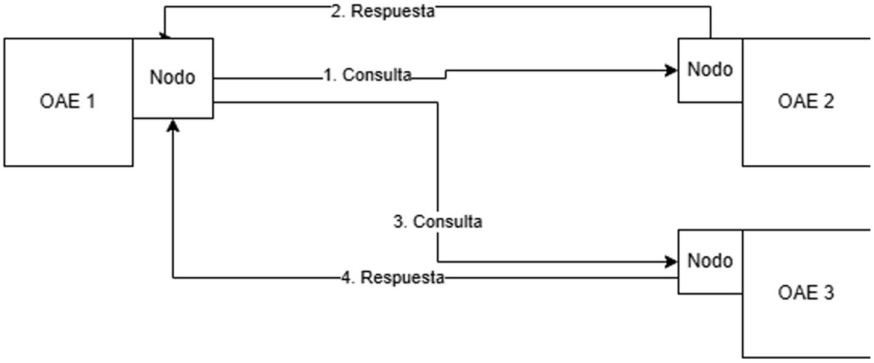
Inicialmente se propone un sistema que recoja la información contenida en el nodo de forma centralizada, previamente almacenada en caso que no sea posible un sistema de consultas transaccional.



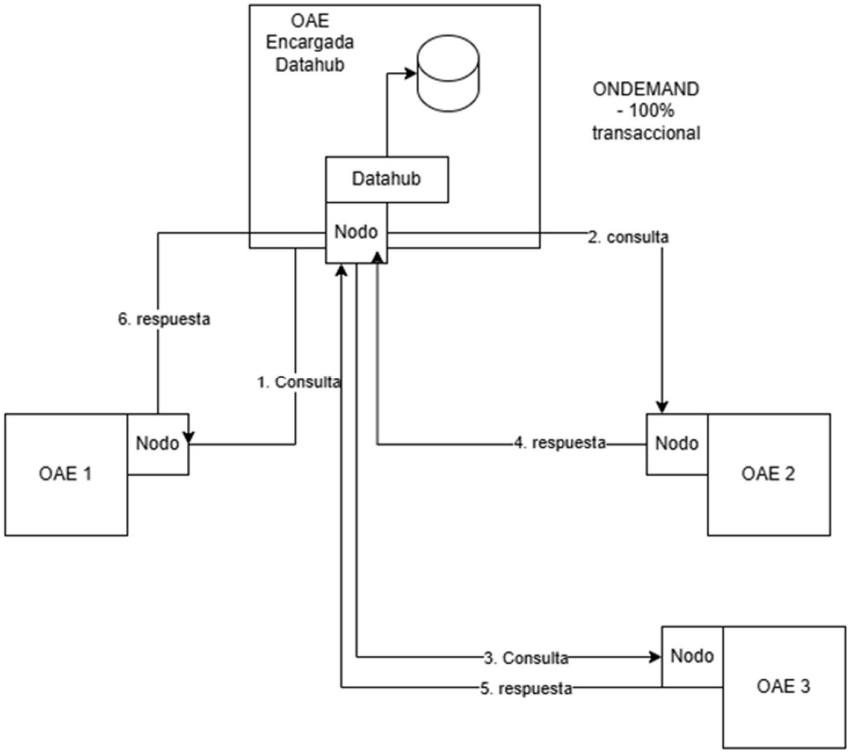
Considerando la posibilidad de un sistema transaccional, se propone un sistema de consultas 100% transaccional, primero independiente del nodo sectorial, lo cual dificulta la centralización de información para la Ficha Única



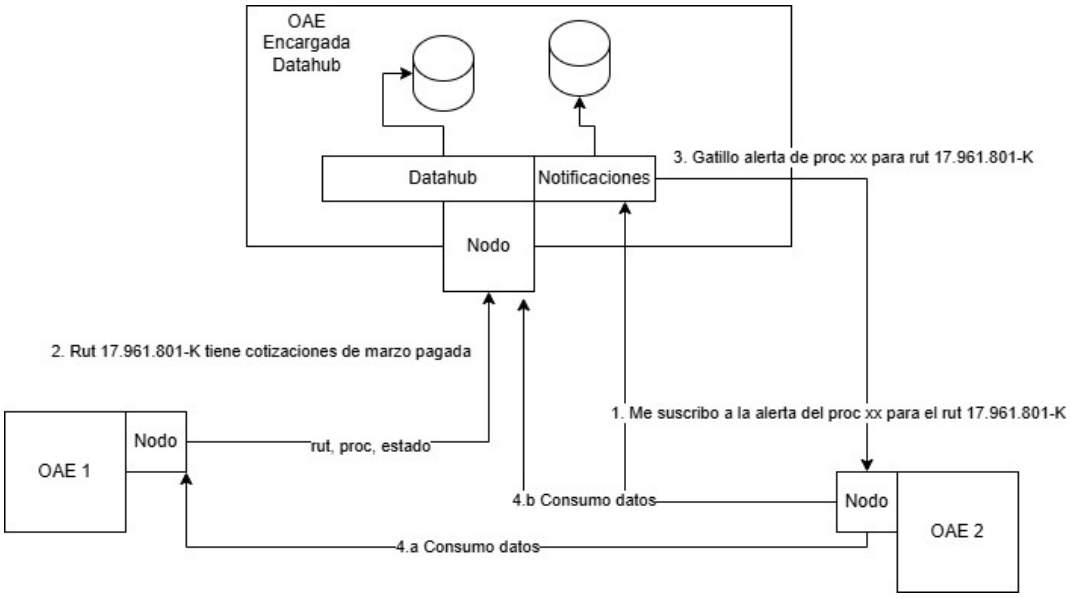
100%
transaccional



Facilitando la centralización, se analiza el sistema transaccional junto con que el intercambio sea a través del Nodo Sectorial, permitiendo almacenar temporalmente la información necesaria para la Ficha Única y la comunicación entre varias instituciones de forma simultánea.



Por último, para mejorar la eficiencia del sistema de interoperabilidad y la proactividad de las OAEs, se incorpora el sistema de notificaciones que permite dar aviso sobre la data que ha sido actualizada por parte de la entidad oferente de la información. Además, esto genera una trazabilidad de la data actualizada.



ANEXO 5: FICHA ÚNICA LABORAL Y PREVISIONAL

A continuación, se muestra la estructura de la ficha que enviaría el Nodo Sectorial. En este caso se supone que la OAE tenga acceso a todas las fuentes de datos que esta puede contener y que los datos de la persona, están validados con el Servicio de Registro Civil e Identificación (SRCEI), lo cual está puesto como la primera entidad/fuente de datos.

- Inicialmente se entrega el Response Header con la información correspondiente al envío del mensaje, específicamente, se entrega uno de los códigos destacados en la estructura a continuación, que representa el estado a nivel general de la información entregada (“Status code”:).
- Después el Payload entrega la petición realizada “OAE.Fuente de dato” (por ejemplo, `"IPS.obtenerresolucionAF"`) y el token de Clave Única que permite acceder a la información con el permiso del ciudadano dueño de la información.
- Siguiente a esa sección, se encuentra la Ficha Única consolidada, la cual entrega las fuentes de información separando inicialmente por la OAE y granularmente por fuente de información.
- Por último, se entrega el estado del envío de información por fuente de dato (**`"serviceStates": {`**), donde se muestran ejemplos de respuesta dentro de cada fuente de información que también están agrupados por OAE.

```
Response Header: {

  "Status": {
    "code": 200,
    "message": "OK - Solicitud exitosa",

    "code": 207,
    "message": "MultiStatus - Algunas fuentes fueron exitosas y otras no",

    "code": 400,
    "message": "Bad Request - JSON mal formado o datos inválidos",

    "code": 401,
    "message": "Unauthorized - No autorizado para acceder al recurso",

    "code": 503,
    "message": "Service Unavailable - Servicio no disponible",
  },

  "Content-Type": application/json
}


//respuesta json

{
  "FichaUnica":{

    "SRCEI": {
      "datosBasicos": {
        "nombres": "STRING",
        "apellidos": "STRING",
        "rut": "STRING",
        "fechaNacimiento": "DATE(YYYY-MM-DD)",
        "comuna": "STRING"
      }
    },
    "IPS": {
      "obtenerResolucionAF": {
        "solicitudId": "NUMERIC",
        "beneficioId": "NUMERIC",
        "descripcion": "STRING",
        "idRepositorio": "NUMERIC",
        "idRepositorioFinal": "NUMERIC",
        "fecCreacionAno": "NUMERIC",
        "fecCreacionMes": "NUMERIC",
        "base64File": "BLOB",
```

```
      "timestamp": "DATETIME()"
    },
    "proximaFechaPagoBeneficios": {
      "runBeneficiario": "NUMERIC",
      "dvBeneficiario": "STRING",
      "proximoPago": [
        {
          "fechaProximoPago": "YYYYMMDD",
          "beneficio": "STRING",
          "formaPago": "STRING",
          "descripcionBeneficio": "STRING"
        }
      ]
    }
  },
  "SP": {
    "cotizacionesPrevisionales": {
      "fechaUltimaCotizacion": "DATE(YYYY-MM-DD)",
      "cotizaciones": [
        {
          "rutAfp": "STRING",
          "periodoCotizado": "DATE(YYYY-MM)",
          "montoCotizado": "NUMERIC",
          "porcentajeCotizado": "NUMERIC",
          "fechaPago": "DATE(YYYY-MM-DD)",
          "montoRemuneracionImponible": "NUMERIC",
          "tipoMovimientoCotizacionObligatoria": "STRING",
          "fondoDestino": "STRING",
          "rutPagadorEmpleador": "NUMERIC"
        }
      ],
      "fechaCorteAfp": "DATE(YYYY-MM-DD)"
    }
  },
  "SUSESO":{
    "ConsultaAfiliacionCaja":{
      "cajas":[
        {
          "nombre": "STRING",
          "fecha_ingreso": "DATE(YYYY-MM-DD)",
          "empleador": "STRING",
          "tipo_afiliacion": "STRING"
        }
      ]
    },
    "ConsultaAfiliacionMutual":{
      "Mutuales":{
        "Mutual":
```

```
        {
            "nombre":"<nombre_mutual>"
        }
      }
    },
    "SIAGFConsultaCausanteSimple":{
      "rutCausante": "STRING",
      "nombreCausante": "STRING",
      "entidadAdministradora": "STRING",
      "fechaReconocimiento": "DATE(YYYY-MM-DD)",
      "tipoBeneficio": "STRING",
      "tipoCausante": "STRING",
      "tipoBeneficiario": "STRING",
      "rutEmpleador": "STRING",
      "nombreEmpleador": "STRING"
    }
  },
  "DT": {
    "registroContratoTrabajo": {
      "idContrato": "NUMERIC",
      "categoriaContrato": "STRING",
      "fechaSuscripcionContrato": "DATE(YYYY-MM-DD)",
      "rutEmpleador": "STRING",
      "rutTrabajador": "STRING",
      "declaracionDiscapacidad": "STRING",
      "declaracionInvalidez": "STRING",
      "funciones": "STRING",
      "estadoId": "NUMERIC",
      "estadoContrato": "STRING",
      "fechaInicioContrato": "DATE(YYYY-MM-DD)"
    },
    "registroTerminoContratoTrabajo": {
      "rutEmpleador": "NUMERIC",
      "dvRutEmpleador": "STRING",
      "fechaInicioRelacionLaboral": "DATE(YYYY-MM-DD)",
      "fechaFinRelacionLaboral": "DATE(YYYY-MM-DD)",
      "fechaRegistro": "DATE(YYYY-MM-DD)",
      "causalTipoTermino": "STRING",
      "comunaDomicilioTrabajador": "STRING",
      "comunaDomicilioEmpleador": "STRING",
      "funciones": "STRING"
    },
    "libroRemuneracionesElectronico": {
      "fechaInicioContrato": "DATE(YYYY-MM-DD)",
      "comunaPrestacionServicios": "STRING",
      "tipoImpuestoRenta": "STRING",
      "codigoTipoJornada": "STRING",
      "afp": "STRING",
```

```
        "ips": "STRING",
        "fonasaIsapre": "STRING",
        "afc": "STRING",
        "ccaf": "STRING",
        "orgAdministradorLey16744": "STRING",
        "nroDiasTrabajados": "NUMERIC",
        "sueldo": "NUMERIC",
        "totalLiquido": "NUMERIC"
      }
    },
    "DIPRECA": {
      "montoDePensiones":{

        "montoPensiones": "number",
        "montoImponible": "number",
        "montoNoImponible": "number",
        "montoLiquido": "number",
        "erogacionMenores65": "number",
        "erogacionMayores65": "number",
        "totalHaberes": "number",
        "totalDescuentos": "number",
        "tipoPension": "string",
        "numeroPension": "number",
        "subCuenta": "number",
        "run": "string",
        "reparticion": "number"
      },
      "asignacionFamiliar":{
        "montoAsignacionFamiliar": "number",
        "cargasSimples": "number",
        "cargasDuplo": "number",
        "nombre": "string",
        "run": "number",
        "dgv": "number",
        "tramo": "string",
        "fechaPago": "string",
        "estado": "string",
        "tipoParentesco": "string"
      }
    }
  },
  "serviceStates": {
    "SRCEI": {
      "datosBasicos":{

        "code": 200,
        "message": "OK - Solicitud exitosa",
```

```
      "code": 400,
      "message": "Bad Request - JSON mal formado o datos inválidos",

      "code": 401,
      "message": "Unauthorized - No autorizado para acceder al recurso",

      "code": 403,
      "message": "Forbidden - Acceso prohibido",

      "code": 404,
      "message": "Not Found - Recurso no encontrado",

      "code": 500,
      "message": "Internal Server Error - Error interno del servidor",

      "code": 503,
      "message": "Service Unavailable - Servicio no disponible",

      "code": 504,
      "message": "Gateway Timeout - Tiempo de espera agotado",
    }
  },
  "IPS":{
    "obtenerResolucionAF":{

      "code": 200,
      "message": "OK - Solicitud exitosa",

      "code": 400,
      "message": "Bad Request - JSON mal formado o datos inválidos",

      "code": 401,
      "message": "Unauthorized - No autorizado para acceder al recurso",

      "code": 403,
      "message": "Forbidden - Acceso prohibido",

      "code": 404,
      "message": "Not Found - Recurso no encontrado",

      "code": 500,
      "message": "Internal Server Error - Error interno del servidor",

      "code": 503,
      "message": "Service Unavailable - Servicio no disponible",

      "code": 504,
      "message": "Gateway Timeout - Tiempo de espera agotado",
```

```
    },
    "proximaFechaPagoBeneficios":{

      "code": 200,
      "message": "OK - Solicitud exitosa",

      "code": 400,
      "message": "Bad Request - JSON mal formado o datos inválidos",

      "code": 401,
      "message": "Unauthorized - No autorizado para acceder al recurso",

      "code": 403,
      "message": "Forbidden - Acceso prohibido",

      "code": 404,
      "message": "Not Found - Recurso no encontrado",

      "code": 500,
      "message": "Internal Server Error - Error interno del servidor",

      "code": 503,
      "message": "Service Unavailable - Servicio no disponible",

      "code": 504,
      "message": "Gateway Timeout - Tiempo de espera agotado",
    }
  },
  "SP":{
    "ultimasCotizacionesPrevisionales":{

      "code": 200,
      "message": "OK - Solicitud exitosa",

      "code": 400,
      "message": "Bad Request - JSON mal formado o datos inválidos",

      "code": 401,
      "message": "Unauthorized - No autorizado para acceder al recurso",

      "code": 403,
      "message": "Forbidden - Acceso prohibido",

      "code": 404,
      "message": "Not Found - Recurso no encontrado",

      "code": 500,
      "message": "Internal Server Error - Error interno del servidor",
```

```
      "code": 503,
      "message": "Service Unavailable - Servicio no disponible",

      "code": 504,
      "message": "Gateway Timeout - Tiempo de espera agotado",
    }
  },
  "SUSESO":{
    "ConsultaAfiliacionCaja":{

      "code": 200,
      "message": "OK - Solicitud exitosa",

      "code": 400,
      "message": "Bad Request - JSON mal formado o datos inválidos",

      "code": 401,
      "message": "Unauthorized - No autorizado para acceder al recurso",

      "code": 403,
      "message": "Forbidden - Acceso prohibido",

      "code": 404,
      "message": "Not Found - Recurso no encontrado",

      "code": 500,
      "message": "Internal Server Error - Error interno del servidor",

      "code": 503,
      "message": "Service Unavailable - Servicio no disponible",

      "code": 504,
      "message": "Gateway Timeout - Tiempo de espera agotado",
    },
    "ConsultaAfiliacionMutual":{

      "code": 200,
      "message": "OK - Solicitud exitosa",

      "code": 400,
      "message": "Bad Request - JSON mal formado o datos inválidos",

      "code": 401,
      "message": "Unauthorized - No autorizado para acceder al recurso",

      "code": 403,
      "message": "Forbidden - Acceso prohibido",
```

```
      "code": 404,
      "message": "Not Found - Recurso no encontrado",

      "code": 500,
      "message": "Internal Server Error - Error interno del servidor",

      "code": 503,
      "message": "Service Unavailable - Servicio no disponible",

      "code": 504,
      "message": "Gateway Timeout - Tiempo de espera agotado",
    },
    "SIAGFConsultaCausanteSimple":{

      "code": 200,
      "message": "OK - Solicitud exitosa",

      "code": 400,
      "message": "Bad Request - JSON mal formado o datos inválidos",

      "code": 401,
      "message": "Unauthorized - No autorizado para acceder al recurso",

      "code": 403,
      "message": "Forbidden - Acceso prohibido",

      "code": 404,
      "message": "Not Found - Recurso no encontrado",

      "code": 500,
      "message": "Internal Server Error - Error interno del servidor",

      "code": 503,
      "message": "Service Unavailable - Servicio no disponible",

      "code": 504,
      "message": "Gateway Timeout - Tiempo de espera agotado",
    }
  },
  "DT":{
    "registroContratoTrabajo":{

      "code": 200,
      "message": "OK - Solicitud exitosa",

      "code": 400,
      "message": "Bad Request - JSON mal formado o datos inválidos",
```

```
    "code": 401,
    "message": "Unauthorized - No autorizado para acceder al recurso",

    "code": 403,
    "message": "Forbidden - Acceso prohibido",

    "code": 404,
    "message": "Not Found - Recurso no encontrado",

    "code": 500,
    "message": "Internal Server Error - Error interno del servidor",

    "code": 503,
    "message": "Service Unavailable - Servicio no disponible",

    "code": 504,
    "message": "Gateway Timeout - Tiempo de espera agotado",
  },
  "registroTerminoContratoTrabajo":{

    "code": 200,
    "message": "OK - Solicitud exitosa",

    "code": 400,
    "message": "Bad Request - JSON mal formado o datos inválidos",

    "code": 401,
    "message": "Unauthorized - No autorizado para acceder al recurso",

    "code": 403,
    "message": "Forbidden - Acceso prohibido",

    "code": 404,
    "message": "Not Found - Recurso no encontrado",

    "code": 500,
    "message": "Internal Server Error - Error interno del servidor",

    "code": 503,
    "message": "Service Unavailable - Servicio no disponible",

    "code": 504,
    "message": "Gateway Timeout - Tiempo de espera agotado",
  },
  "libroRemuneracionesElectronico":{

    "code": 200,
```

```
        "message": "OK - Solicitud exitosa",

        "code": 400,
        "message": "Bad Request - JSON mal formado o datos inválidos",

        "code": 401,
        "message": "Unauthorized - No autorizado para acceder al recurso",

        "code": 403,
        "message": "Forbidden - Acceso prohibido",

        "code": 404,
        "message": "Not Found - Recurso no encontrado",

        "code": 500,
        "message": "Internal Server Error - Error interno del servidor",

        "code": 503,
        "message": "Service Unavailable - Servicio no disponible",

        "code": 504,
        "message": "Gateway Timeout - Tiempo de espera agotado",
      },
      "registroTerminoContratoTrabajo":{

        "code": 200,
        "message": "OK - Solicitud exitosa",

        "code": 400,
        "message": "Bad Request - JSON mal formado o datos inválidos",

        "code": 401,
        "message": "Unauthorized - No autorizado para acceder al recurso",

        "code": 403,
        "message": "Forbidden - Acceso prohibido",

        "code": 404,
        "message": "Not Found - Recurso no encontrado",

        "code": 500,
        "message": "Internal Server Error - Error interno del servidor",

        "code": 503,
        "message": "Service Unavailable - Servicio no disponible",

        "code": 504,
        "message": "Gateway Timeout - Tiempo de espera agotado",
```

```
    }
  },
  "DIPRECA": {
    "montoDePensiones":{

      "code": 200,
      "message": "OK - Solicitud exitosa",

      "code": 400,
      "message": "Bad Request - JSON mal formado o datos inválidos",

      "code": 401,
      "message": "Unauthorized - No autorizado para acceder al recurso",

      "code": 403,
      "message": "Forbidden - Acceso prohibido",

      "code": 404,
      "message": "Not Found - Recurso no encontrado",

      "code": 500,
      "message": "Internal Server Error - Error interno del servidor",

      "code": 503,
      "message": "Service Unavailable - Servicio no disponible",

      "code": 504,
      "message": "Gateway Timeout - Tiempo de espera agotado",
    },
    "asignacionFamiliar":{

      "code": 200,
      "message": "OK - Solicitud exitosa",

      "code": 400,
      "message": "Bad Request - JSON mal formado o datos inválidos",

      "code": 401,
      "message": "Unauthorized - No autorizado para acceder al recurso",

      "code": 403,
      "message": "Forbidden - Acceso prohibido",

      "code": 404,
      "message": "Not Found - Recurso no encontrado",

      "code": 500,
      "message": "Internal Server Error - Error interno del servidor",
```

```
        "code": 503,
        "message": "Service Unavailable - Servicio no disponible",

        "code": 504,
        "message": "Gateway Timeout - Tiempo de espera agotado",
      }
    }
  }
}
```