

Documento de Arquitectura Mi Mutual, Sistema de Previsión, Asistencia y Solidaridad, Coomeva, STEF - Coomeva

Mi Mutual Coomeva - Mi Mutual, Sistema de Previsión, Asistencia y Solidaridad, Coomeva

Versión del producto 1.3007b3d de 25 Oct 2023

Presentado a

STEF - Coomeva

Fecha

25 Oct 2023

Autores

- **Equipo arquitectura STEF-COOMV.**

·  Usuario [e_hwong](#)

Arquitecto, Stefanini

✉ — Enviar mensajes a Equipo arquitectura STEF-COOMV. <e_hwong@stefanini.com>.

Objetivo del Documento

Descripción de los productos del trabajo de arquitectura del proyecto MI MUTUAL de la Coomeva, Contrato XXX-2023. El principal propósito de este documento es informar de las decisiones sobre la disposición lógica y física de las partes del sistema. Por tanto, el documento contiene información estratégica, siendo en algunos casos el diseño detallado. Puntualmente, el documento refleja decisiones sobre la plataforma tecnológica seleccionada, así como consideraciones importantes para el diseño y desarrollo, con procura de garantizar una solución técnicamente viable y óptima para el proyecto.

Control de Cambios

Tema	Mi Mutual Coomeva Mi Mutual, Sistema de Previsión, Asistencia y Solidaridad, Coomeva
Palabras clave	SIU, Stefanini, Coomeva, Análisis de brecha, GAP, Comparativa
Autor	
Fuente	
Versión	1.3007b3d del 25 Oct 2023
Vínculos	N003a Vista Segmento Coomeva SIU

Contenidos

Introducción

Propósito

Este documento tiene como propósito presentar la arquitectura del aplicativo Mi Mutual para STEF - Coomeva, según los requerimientos definidos durante la etapa de preventa y luego detallados en las historias de usuario.

La arquitectura será una guía para que el diseño y la implementación de los componentes que conforman la solución sean cobijados bajo lineamientos y premisas bien definidos, permitiendo a los elementos del sistema interactuar entre sí de forma coherente. La arquitectura será tomada como un diseño estratégico que establece restricciones globales para el diseño, define un marco inicial de trabajo para la implementación de los requerimientos funcionales y no funcionales.

La definición arquitectónica de este proyecto será un proceso evolutivo. Por tanto, la información de este documento es susceptible a cambios a medida que se vayan agregando nuevas funcionalidades o requisitos al sistema.

Uno de los principales propósitos de este documento es hacer una representación de las decisiones de disposición lógica y física de las partes del sistema; por tanto, es un diseño estratégico, no un diseño detallado. Puntualmente, refleja decisiones sobre la plataforma tecnológica seleccionada, así como consideraciones importantes para el diseño y desarrollo, con procura de garantizar una solución técnicamente viable y óptima para el proyecto.

Restricciones Principales de Arquitectura

Informamos de las restricciones que hacen parte de Mi Mutual, y por tanto, a considerar en el ejercicio de arquitectura del presente proyecto.

Lista de restricciones de Mi Mutual, 2023.

1. Disponibilidad. Se requiere que el sistema esté disponible 7x24, el servicio prestado al cliente no se limita a horarios de oficina pues las compras pueden darse en cualquier momento
2. Escalabilidad. Se requiere que el sistema pueda llegar a atender hasta 1.000 clientes, para esto se requiere que el sistema se pueda extender horizontalmente de tal manera que pueda tener instalado en varios servidores para atender esta cantidad de usuarios. Todas las aplicaciones desarrolladas podrán ser escaladas horizontalmente para atender la demanda relacionada con el crecimiento de la empresa.
3. Reutilización. Se requiere que el sistema permita reutilizar sus componentes para prestar el mismo servicio a otras aplicaciones de la compañía. Para esto se va a desarrollar la aplicación utilizando servicios, separados y con asignación de responsabilidades, propias, de tal manera de que, si se requiere exponer servicios web sobre estas funcionalidades, no requiere cambios en la aplicación.
4. Autenticación. Autenticación es el proceso para determinar que alguien o un sistema es quien dice ser. Uso de estándar Oauth2 y JSON Web Token - JWT, para gestión de autenticación de servicios de la aplicación.
5. Autorización. Autorización se refiere a la validación que realiza un sistema para determinar si un usuario puede usar cierta funcionalidad. Uso de API de seguridad de Spring (spring-security) + Oauth2
6. Interoperabilidad – Movilidad. Interoperabilidad se refiere a la habilidad de un sistema de interactuar y comunicarse con sistemas heterogéneos a través de interfaces completamente definidas. Uso de estándar de web services REST + JSON.
7. Facilidad de Uso. Se refiere a la facilidad con que las personas pueden utilizar el sistema porque facilitan la lectura de los textos, descargan rápidamente la información y presentan funciones y menús sencillos, por lo que el usuario encuentra satisfechas sus consultas y cómodo su uso.
8. Verificación (QA). Es la capacidad del producto software que hace posible que el software modificado sea probado.
9. Estándares. Los estándares seleccionados por la solución de este proyecto, (Mi Mutual, Sistema de Previsión, Asistencia y Solidaridad, Coomeva, están determinados por el uso de las plataformas específicas determinadas por la implementación (desarrollo del software).

Restricciones Secundarias

Otras restricciones a detallar.

1. Repositorio de datos.
2. Memoria, disco, CPU.
3. Requerimientos de rendimiento.

Requisitos de Arquitectura (no funcional)

Entendemos como requisitos de arquitectura aquellos requerimientos no visibles pero estructurales, medibles, y que impactan al funcionamiento, desarrollo y mantenimiento de la solución Mi Mutual, objeto de este proyecto, Mi Mutual Coomeva.

Definiremos estos requisitos de la solución a tener en cuenta al momento del desarrollo.

Requerimientos generales

1. **Parametrización.** Crear desarrollos parametrizables necesarios para permitir la administración de la información de uso general.
2. **Interoperabilidad.** Crear desarrollos de Mi Mutual interoperables con otros sistemas de información de la entidad según requerimientos de los procesos.
3. **Diseño.** Los desarrollos complementarios deben responder a los criterios de bajo acoplamiento y alta cohesión.
4. **Reglas de negocio.** Las soluciones deben disponer de todas las validaciones y controles que garanticen la calidad, seguridad y unicidad de la información.
5. Para los casos que aplique, la solución debe contar con una integración con el servicio de correo de la Entidad.
6. Todos los desarrollos complementarios serán en su totalidad propiedad de la entidad, para lo cual la entidad podrá modificar y/o actualizar a futuro los procesos modelados, acorde a las necesidades; por tanto, deberán entregarse los derechos intelectuales y patrimoniales como parte de la documentación y el código fuente que corresponda.

Requisitos Particulares de Arquitectura (no funcional)

Consistencia Mi Mutual (lógica)

Tabla 1: Requisito no. 1, Desarrollo Mi Mutual, Consistencia.

Requisito	Extensibilidad Mi Mutual
Descripción	Unifica las entidades de negocio Coomeva, entre las que se incluyen a conciliaciones, publicaciones de relatoría, resoluciones, en artefactos reutilizables. Distinto de que estas entidades (y su lógica de negocio) estén dispersos entre los sistemas del Mi Mutual, estarán concentradas en un único artefacto correspondiente.
Calidad sistemática	La consistencia persigue que el resultado de la lógica de negocio sea la misma entre los módulos del Mi Mutual migrado. Esto redunda a mantenibilidad y gestión: tiende a tener un solo punto de cambio y dificulta la transferencia de dependencias implícitas a otros procesos.

Mantenibilidad Mi Mutual

Tabla 2: Requisito no. 2, Mantenibilidad Mi Mutual.

Requisito	Mantenibilidad Mi Mutual
Descripción	Evitar las dependencias transitivas de los módulos misionales del Mi Mutual a componentes y sistemas de terceros o submódulos no misionales.
Calidad sistemática	La mantenibilidad por control de dependencias que optimiza el diseño Desarrollo Mi Mutual está dada por el control de cambios no programados sobre los componentes misionales del Mi Mutual (corrupción de componentes). Ver Patrón de Diseño Desarrollo Mi Mutual, más adelante en el documento.

Extensibilidad Mi Mutual

Tabla 3: Requisito no. 3, Desarrollo Mi Mutual, Flexibilidad.

Requisito	Extensibilidad Mi Mutual
Descripción	Concentración de los componentes de negocio, misionales, del Mi Mutual protegidos de cambios provenientes de otros sistemas. Ver Patrón de Diseño Desarrollo Mi Mutual, más adelante en el documento.
Calidad sistemática	La extensibilidad que optimiza el diseño Desarrollo Mi Mutual está dada por el intercambio de submódulos no misionales, como el gestor documental, sin afectación de los componentes misionales que este diseño protege.

Arq MiMutual. 1. Contexto

Mi Mutual. Coomeva, 2023.

Contexto Mi Mutual: Áreas negocio, componente central Mi Mutual, servicios y funciones.

versión 0.2.1

Contexto Mi Mutual Central

El sistema principal de fondo Mi Mutual Central es la composición de las funciones de negocio de la Unidad de Solidaridad de Coomeva. Las funciones de negocio referidas, como Gestión Beneficiarios, Certificados, Gestión Beneficiarios, aparecen dentro del componente principal en la imagen.

Este entregable documenta los diferentes módulos y componentes que hacen parte de la estructura de una aplicación en Angular 12 y como es su interacción para conformar una arquitectura robusta y escalable para aplicaciones de gran tamaño.

Las librerías Spring Boot Security y Spring Boot Oauth2 proveen características de seguridad entre Vista (Angular 2) y Controlador. Estas son responsables de que únicamente permita el acceso si se está autenticado. Además, para realizar el proceso de autenticación se delega a la aplicación SISPRO (Coomeva) que funciona como un servidor de autenticación.

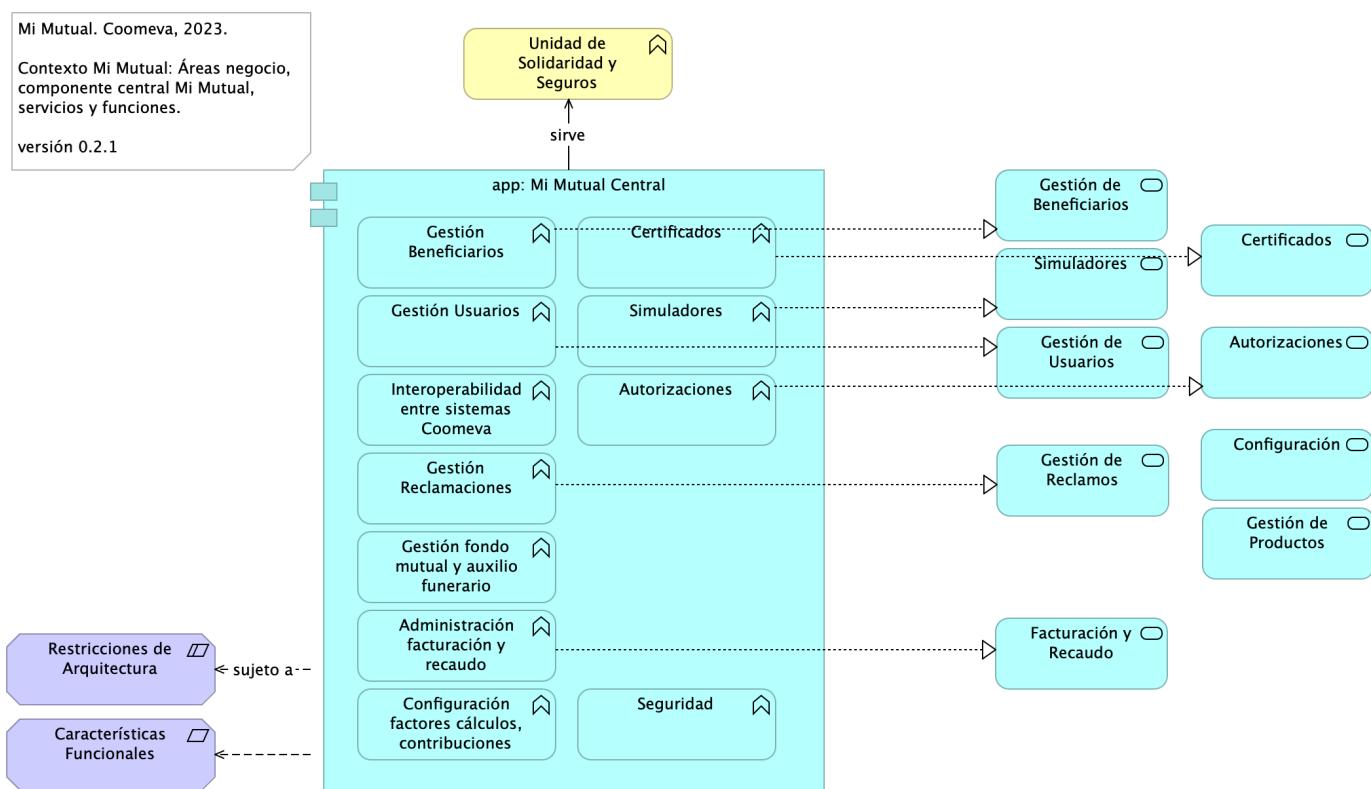


Imagen 1: Arq MiMutual. 1. Contexto

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 4: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
Administración facturación y recaudo	Application Function	Administración de la facturación y recaudo diario de los productos	
Autorizaciones	Application Function	Autorizaciones: Administración de peticiones de autorización y sus correspondientes aprobaciones mediante el servicio del flujo de procesos	

Nombre	Tipo	Documentación	Propiedad
Autorizaciones	Application Service	<p>Autorizaciones: Administración de peticiones de autorización y sus correspondientes aprobaciones usando el servicio del flujo de procesos.</p>	
Características Funcionales	Requirement	<p>## Características Funcionales Mi Mutual</p> <p>1. Gestión de productos del fondo mutual y auxilio funerario que involucran a sus coberturas 1. Administración de la facturación y recaudo diario de los productos 1. Gestión de Reclamaciones (Indemnización): Permite realizar la gestión, seguimiento y pago o negación de las diferentes reclamaciones de acuerdo a las coberturas y los productos que se encuentren dentro del portafolio del Asociado. 1. Gestión de Beneficiarios: Permite administrar la información relacionada con los beneficiarios del Asociado, permitiendo ejecutar operaciones de consulta, inserción y modificación. 1. Gestión de Usuarios: Administración de la información relacionada con los usuarios del sistema. Este componente se comunica con el servicio unificado de autenticación y autorización que devuelve los permisos que un usuario posee sobre las opciones que proporciona el sistema. 1. Integración con otros sistemas para facilitar los procesos de vinculación, retiro, reactivación o fallecimiento de asociados. 1. Configuración o parametrización de factores para realizar los cálculos de las contribuciones de los asociados a la Cooperativa para cada uno de los productos adquiridos.</p>	
Certificados	Application Function	<p>Certificados: Permite la generación de los certificados de valores de protección y contribuciones pagadas, de retención en la fuente, de pagos de perseverancia y de cobertura de auxilio funerario.</p>	
Certificados	Application Service	<p>Certificados: Permite la generación de los certificados de valores de protección y contribuciones pagadas, de retención en la fuente, de pagos de perseverancia y de cobertura de auxilio funerario.</p>	
Configuración	Application Service	<p>Configuración o parametrización de factores para realizar los cálculos de las contribuciones de los asociados a la Cooperativa para cada uno de los productos adquiridos.</p>	
Configuración factores cálculos, contribuciones	Application Function	<p>1. Configuración o parametrización de factores para realizar los cálculos de las contribuciones de los asociados a la Cooperativa para cada uno de los productos adquiridos.</p>	

Nombre	Tipo	Documentación	Propiedad
Facturación y Recaudo	Application Service	Administración de la facturación y recaudo diario de los productos	
Gestión Beneficiarios	Application Function	Gestión de Beneficiarios: Permite administrar la información relacionada con los beneficiarios del Asociado, permitiendo ejecutar operaciones de consulta, inserción y modificación.	
Gestión Reclamaciones	Application Function	Gestión de Reclamaciones (Indemnización): Permite realizar la gestión, seguimiento y pago o negación de las diferentes reclamaciones de acuerdo a las coberturas y los productos que se encuentren dentro del portafolio del Asociado.	
Gestión Usuarios	Application Function	Gestión de Usuarios: Administración de la información relacionada con los usuarios del sistema. Este componente se comunica con el servicio unificado de autenticación y autorización que devuelve los permisos que un usuario posee sobre las opciones que proporciona el sistema.	
Gestión de Beneficiarios	Application Service	Gestión de Beneficiarios: Permite administrar la información relacionada con los beneficiarios del Asociado, permitiendo ejecutar operaciones de consulta, inserción y modificación	
Gestión de Productos	Application Service	Gestión de productos del fondo mutual y auxilio funerario que involucran lo relacionado a las siguientes coberturas: * Fondo de Solidaridad: Incapacidades temporales, Incapacidades Permanentes (total, parcial), Perseverancia 60, 62, 65, 70 años, Perseverancias Anticipadas, Fallecimiento Asociado (Auxilio por muerte), Desempleo, Disminución de ingresos y enfermedades graves; Rentas por hospitalización, Enfermedades de Alto Costo, Pólizas de seguros personales y patrimoniales, Planes educativos, Segunda opinión médica, Asistencias. * Auxilio Funerario: Fallecimiento de familiares directos (inscritos) del Asociado.	
Gestión de Reclamos	Application Service	Gestión de Reclamaciones (Indemnización): Permite realizar la gestión, seguimiento y pago o negación de las diferentes reclamaciones de acuerdo a las coberturas y los productos que se encuentren dentro del portafolio del Asociado	
Gestión de Usuarios	Application Service	Gestión de Usuarios: Administración de la información relacionada con los usuarios del sistema. Este componente se comunica con el servicio unificado de autenticación y autorización que devuelve los permisos que un usuario posee sobre las opciones que proporciona el sistema.	

Nombre	Tipo	Documentación	Propiedad
Gestión fondo mutual y auxilio funerario	Application Function	Gestión de productos del fondo mutual y auxilio funerario que involucran a sus coberturas	
Interoperabilidad entre sistemas Coomeva	Application Function	Integración con otros sistemas para facilitar los procesos de vinculación, retiro, reactivación o fallecimiento de asociados.	
Restricciones de Arquitectura	Constraint	<p>## Restricciones de Arquitectura (Atributos)</p> <p>1. Disponibilidad. Se requiere que el sistema esté disponible 7 X 24, el servicio prestado al cliente no se limita a horarios de oficina pues las compras pueden darse en cualquier momento</p> <p>1. Escalabilidad. Se requiere que el sistema pueda llegar a atender hasta 1.000 clientes, para esto se requiere que el sistema se pueda extender horizontalmente de tal manera que pueda tener instalado en varios servidores para atender esta cantidad de usuarios. Todas las aplicaciones desarrolladas podrán ser escaladas horizontalmente para atender la demanda relacionada con el crecimiento de la empresa.</p> <p>1. Reutilización. Se requiere que el sistema permita reutilizar sus componentes para prestar el mismo servicio a otras aplicaciones de la compañía. Para esto se va a desarrollar la aplicación utilizando servicios, separados y con asignación de responsabilidades, propias, de tal manera de que, si se requiere exponer servicios web sobre estas funcionalidades, no requiere cambios en la aplicación.</p> <p>1. Autenticación. Autenticación es el proceso para determinar que alguien o un sistema es quien dice ser. Uso de estándar Oauth2 y JSON Web Token - JWT, para gestión de autenticación de servicios de la aplicación.</p> <p>1. Autorización. Autorización se refiere a la validación que realiza un sistema para determinar si un usuario puede usar cierta funcionalidad. Uso de API de seguridad de Spring (spring-security) + Oauth2</p> <p>1. Interoperabilidad - Movilidad. Interoperabilidad se refiere a la habilidad de un sistema de interactuar y comunicarse con sistemas heterogéneos a través de interfaces completamente definidas. Uso de estándar de web services REST + JSON.</p> <p>1. Facilidad de Uso. Se refiere a la facilidad con que las personas pueden utilizar el sistema porque facilitan la lectura de los textos, descargan rápidamente la información y presentan funciones y menús sencillos, por lo que el usuario encuentra satisfechas sus consultas y cómodo su uso.</p> <p>1. Verificación (QA). Es la capacidad del producto software que hace posible que el software modificado sea probado.</p>	

Nombre	Tipo	Documentación	Propiedad
Seguridad	Application Function		
Simuladores	Application Function	Simuladores: Funcionalidades que permiten generar las simulaciones de los diferentes planes o modificaciones (incrementos y disminuciones) a los productos del Asociado.	
Simuladores	Application Service	Simuladores: Funcionalidades que permiten generar las simulaciones de los diferentes planes o modificaciones (incrementos y disminuciones) a los productos del Asociado.	
Unidad de Solidaridad y Seguros	Business Function	Unidad de Solidaridad y Seguros de la Cooperativa	
app: Mi Mutual Central	Application Component	Antes SIPAS, Mi Mutual es una aplicación web compuesta por distintos módulos de software con arreglo a todas las actividades necesarias que soportan la operación de los productos y servicios que ofrece la Unidad de Solidaridad y Seguros de la Cooperativa.	

Arq MiMutual. 2. Contenedores

Mi Mutual. Coomeva, 2023.

Organización de componentes principales, Mi Mutual Central. Roles de componentes, separación responsabilidades.

versión 0.4.1

La organización de componentes utilizada Mi Mutual, impulsada por Spring Web, antepone como interfaz de uso un API REST. La interfaz se articula con tres componentes utilitarios: Controller, Service y Repository, los cuales están mediados por el componente misional, Mi Mutual, en la imagen.

Esta decisión de organización de los componentes de Mi Mutual, incluyendo al misional del mismo nombre, permite estructurar la aplicación de una manera ordenada y, en línea con las restricciones de arquitectura exigidas al sistema, facilita la efectividad de las extensiones y el mantenimiento.

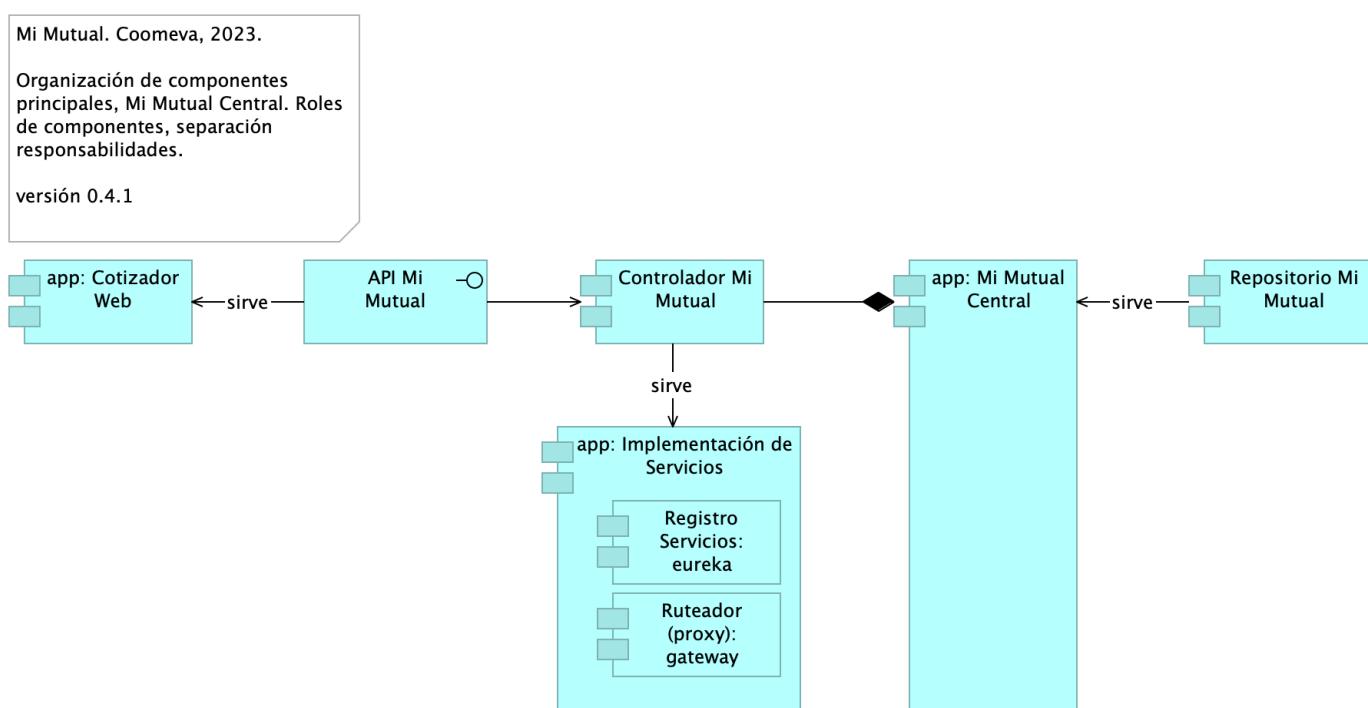


Imagen 2: Arq MiMutual. 2. Contenedores

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 5: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
API Mi Mutual	Application Interface		
Controlador Mi Mutual	Application Component	Los componentes de este tipo se encargan de controlar los servicios rest de la aplicación, además en estos componentes se define la forma como se reciben y envían los datos de los servicios rest y la seguridad de cada uno de los métodos.	
Registro Servicios: eureka	Application Component	Eureka: Contiene todas las funcionalidades relacionadas con registrar y localizar microservicios existentes, informar de su localización, su estado y datos relevantes de cada uno de ellos.	
Repositorio Mi Mutual	Application Component	Antes SIPAS, Mi Mutual es una aplicación web compuesta por distintos módulos de software con arreglo a todas las actividades necesarias que soportan la operación de los productos y servicios que ofrece la Unidad de Solidaridad y Seguros de la Cooperativa. Para el manejo de la persistencia de datos se utilizará Spring Data el cual se apoya en la especificación de JPA y en la implementación de HIBERNATE además de complementar esta capa de persistencia con nuevas funcionalidades que facilitan el acceso a datos.	
Ruteador (proxy): gateway	Application Component	Gateway: Contiene todas las funcionalidades relacionadas con un proxy inverso que reenvía las llamadas relevantes a otros servicios.	
app: Cotizador Web	Application Component	pkg: MiMutualWeb	
app: Implementación de Servicios	Application Component	Los componentes de este tipo se encargan de controlar y almacenar toda la lógica del negocio, validaciones y todo lo referente a procesamiento de datos.	
app: Mi Mutual Central	Application Component	Antes SIPAS, Mi Mutual es una aplicación web compuesta por distintos módulos de software con arreglo a todas las actividades necesarias que soportan la operación de los productos y servicios que ofrece la Unidad de Solidaridad y Seguros de la Cooperativa.	

Arq MiMutual. 3. Dominios

Mi Mutual. Coomeva, 2023.

Servicios trasversales Mi Mutual. Estado Actual.

versión 0.1

La división por dominios busca facilitar la administración los servicios de la plataforma Mi Mutual que son comunes entre aplicaciones de Mi Mutual, tales como Asociados, Reclamaciones, Protecciones y otros servicios trasversales como Utilidades, Reglas de negocio, Procesos de negocio (BPM),

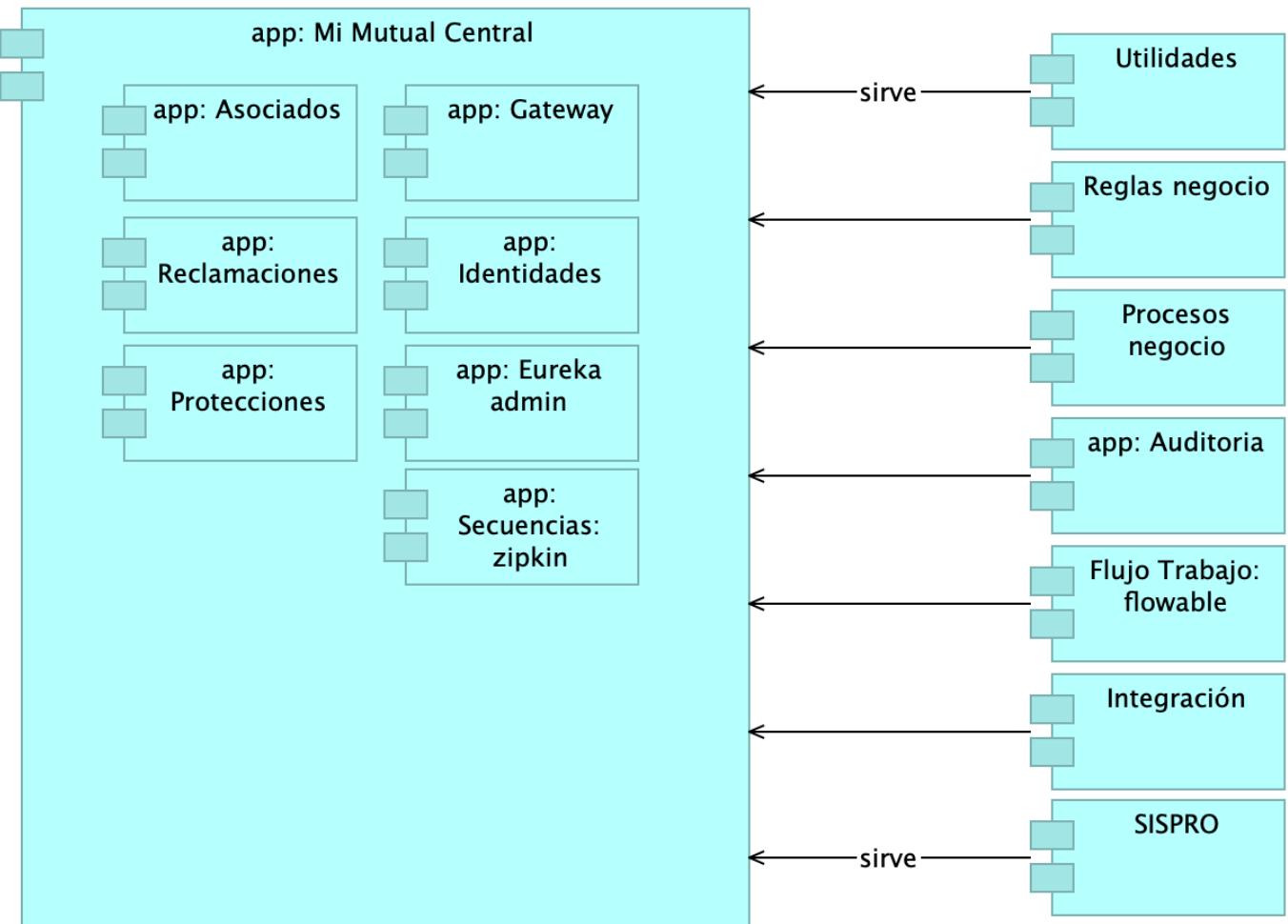
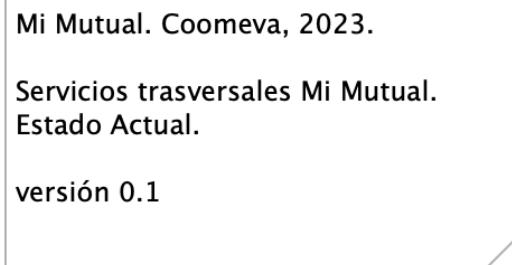


Imagen 3: Arq MiMutual. 3. Dominios

Fuente: *Repositorio arquitectura Mi Mutual (2023)*

Catálogo de Elementos

Tabla 6: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
Flujo Trabajo: flowable	Application Component	Contiene todas las funcionalidades relacionadas con el motor de BPM Flowable, como gestión de tareas, instancias de nuevos procesos y asignación de tareas.	
Integración	Application Component	Contiene todas las funcionalidades relacionadas con integraciones a otros servicios y otras bases de datos.	

Nombre	Tipo	Documentación	Propiedad
Procesos negocio	Application Component	Contiene todas las funcionalidades relacionadas con los flujos de JBPm, actualmente se hace solo para acceso a datos de la base de datos de JBPm.	
Reglas negocio	Application Component	Contiene todas las funcionalidades relacionadas con la validación de reglas usadas en otros microservicios.	
SISPRO	Application Component	Contiene todas las funcionalidades relacionadas con la autenticación y autorización al sistema Mi mutual (Este componente se adopta a la arquitectura de microservicios de MiMutual)	
Utilidades	Application Component	Contiene todas las funcionalidades útiles y trasversales a los microservicios, como envío de correos, generación de archivos Excel, PDF desde Jasper y consulta de parámetros.	
app: Asociados	Application Component	Contiene todas las funcionalidades relacionadas con consulta y creación de asociados y beneficiarios.	
app: Auditoria	Application Component	Contiene todas las funcionalidades relacionadas con el almacenamiento de la auditoría de las peticiones de la aplicación.	
app: Eureka admin	Application Component	Contiene todas las funcionalidades relacionadas con registrar y localizar microservicios existentes, informar de su localización, su estado y datos relevantes de cada uno de ellos.	
app: Gateway	Application Component	Contiene todas las funcionalidades relacionadas con un proxy inverso que reenvía las llamadas relevantes a otros servicios.	
app: Identidades	Application Component	Contiene todas las funcionalidades relacionadas con la gestión de los archivos de propiedades de los microservicios (Esta en construcción y no se ha integrado).	
app: Mi Mutual Central	Application Component	Antes SIPAS, Mi Mutual es una aplicación web compuesta por distintos módulos de software con arreglo a todas las actividades necesarias que soportan la operación de los productos y servicios que ofrece la Unidad de Solidaridad y Seguros de la Cooperativa.	
app: Protecciones	Application Component	Contiene todas las funcionalidades relacionadas con la gestión y configuración de productos y protecciones.	
app: Reclamaciones	Application Component	Contiene todas las funcionalidades relacionadas con la gestión de reclamaciones, liquidaciones y pagos.	
app: Secuencias: zipkin	Application Component	Contiene todas las funcionalidades relacionadas con la generación de IDs para la trazabilidad de los logs.	

Arq MiMutual. 4. Aplicación

Mi Mutual. Coomeva, 2023.

Organización de componentes de aplicación Mi Mutual. Estado Actual. Segmentos (1) frontal, (2) servicios, (3) central/negocio Mi Mutual, (4) infraestructura.

versión 0.4.1

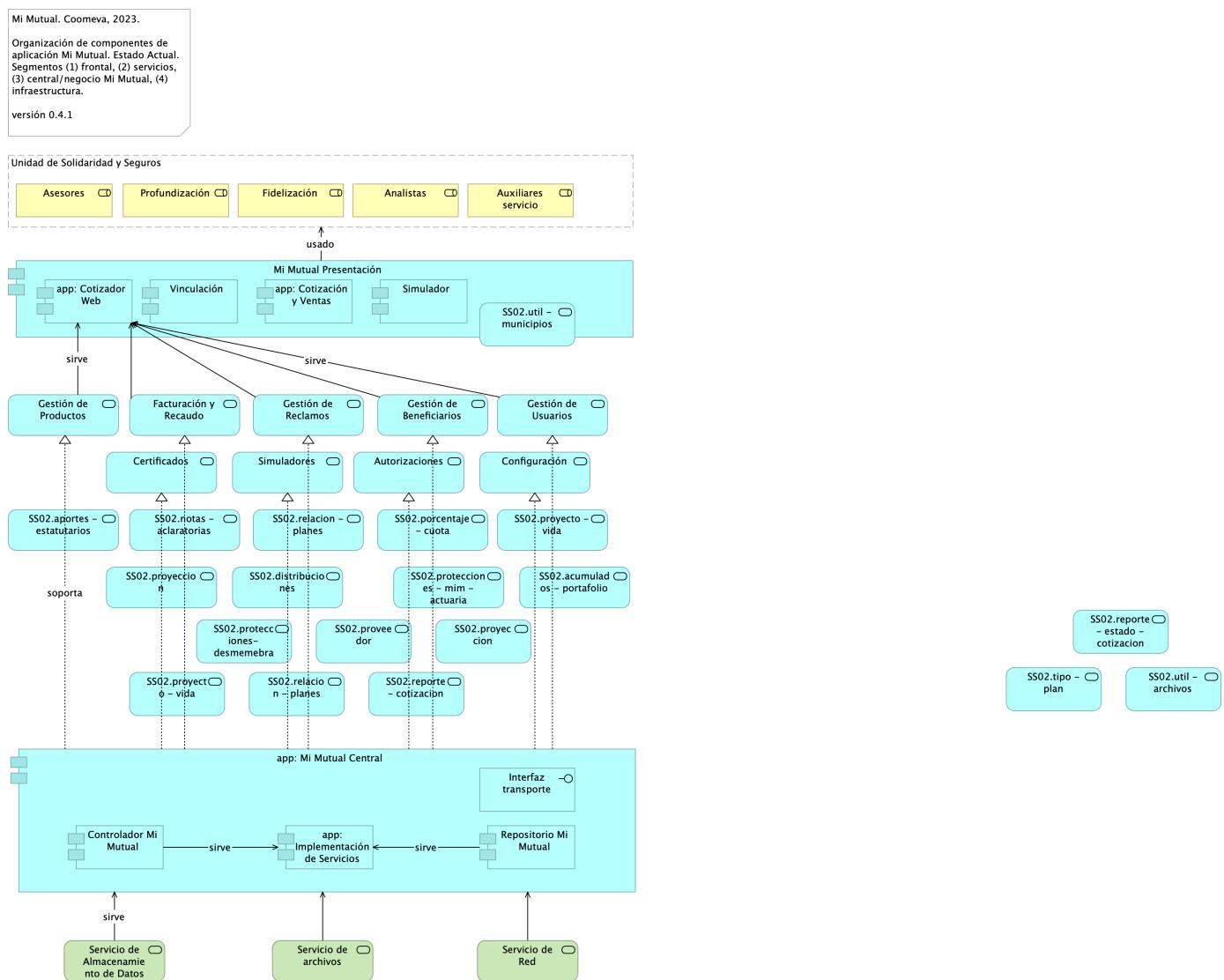


Imagen 4: Arq MiMutual. 4. Aplicación

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 7: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
Analistas	Business Role	Analistas y auxiliares de servicio regional y nacional, agentes del centro de contacto, auditores médicos, analistas de operaciones (aseguramiento y facturación) y jefes.	
Asesores	Business Role	Asesores integrales	
Autorizaciones	Application Service	Autorizaciones: Administración de peticiones de autorización y sus correspondientes aprobaciones usando el servicio del flujo de procesos.	

Nombre	Tipo	Documentación	Propiedad
Auxiliares servicio	Business Role	Analistas y auxiliares de servicio regional y nacional, agentes del centro de contacto, auditores médicos, analistas de operaciones (aseguramiento y facturación) y jefes.	
Certificados	Application Service	Certificados: Permite la generación de los certificados de valores de protección y contribuciones pagadas, de retención en la fuente, de pagos de perseverancia y de cobertura de auxilio funerario.	
Configuración	Application Service	Configuración o parametrización de factores para realizar los cálculos de las contribuciones de los asociados a la Cooperativa para cada uno de los productos adquiridos.	
Controlador Mi Mutual	Application Component	Los componentes de este tipo se encargan de controlar los servicios rest de la aplicación, además en estos componentes se define la forma como se reciben y envían los datos de los servicios rest y la seguridad de cada uno de los métodos.	
Facturación y Recaudo	Application Service	Administración de la facturación y recaudo diario de los productos	
Fidelización	Business Role	Ejecutivos de Fidelización	
Gestión de Beneficiarios	Application Service	Gestión de Beneficiarios: Permite administrar la información relacionada con los beneficiarios del Asociado, permitiendo ejecutar operaciones de consulta, inserción y modificación	
Gestión de Productos	Application Service	Gestión de productos del fondo mutual y auxilio funerario que involucran lo relacionado a las siguientes coberturas: * Fondo de Solidaridad: Incapacidades temporales, Incapacidades Permanentes (total, parcial), Perseverancia 60, 62, 65, 70 años, Perseverancias Anticipadas, Fallecimiento Asociado (Auxilio por muerte), Desempleo, Disminución de ingresos y enfermedades graves; Rentas por hospitalización, Enfermedades de Alto Costo, Pólizas de seguros personales y patrimoniales, Planes educativos, Segunda opinión médica, Asistencias. * Auxilio Funerario: Fallecimiento de familiares directos (inscritos) del Asociado.	
Gestión de Reclamos	Application Service	Gestión de Reclamaciones (Indemnización): Permite realizar la gestión, seguimiento y pago o negación de las diferentes reclamaciones de acuerdo a las coberturas y los productos que se encuentren dentro del portafolio del Asociado	

Nombre	Tipo	Documentación	Propiedad
Gestión de Usuarios	Application Service	Gestión de Usuarios: Administración de la información relacionada con los usuarios del sistema. Este componente se comunica con el servicio unificado de autenticación y autorización que devuelve los permisos que un usuario posee sobre las opciones que proporciona el sistema.	
Interfaz transporte	Application Interface	Feign Client. Integración con otros sistemas para facilitar los procesos de vinculación, retiro, reactivación o fallecimiento de asociados.	
Mi Mutual Presentación	Application Component		
Profundización	Business Role	Ejecutivos de Profundización	
Repositorio Mi Mutual	Application Component	Antes SIPAS, Mi Mutual es una aplicación web compuesta por distintos módulos de software con arreglo a todas las actividades necesarias que soportan la operación de los productos y servicios que ofrece la Unidad de Solidaridad y Seguros de la Cooperativa. Para el manejo de la persistencia de datos se utilizará Spring Data el cual se apoya en la especificación de JPA y en la implementación de HIBERNATE además de complementar esta capa de persistencia con nuevas funcionalidades que facilitan el acceso a datos.	
SS02.acumulados - portafolio	Application Service		
SS02.aportes - estatutarios	Application Service		
SS02.distribuciones	Application Service		
SS02.notas - aclaratorias	Application Service		
SS02.porcentaje - cuota	Application Service		
SS02.protecciones - mim - actuaria	Application Service		
SS02.protecciones- desmembracion - accidente	Application Service		
SS02.proveedor	Application Service		
SS02.proyeccion	Application Service		
SS02.proyecto - vida	Application Service		
SS02.relacion - planes	Application Service		
SS02.reporte - cotizacion	Application Service		
SS02.reporte - estado - cotizacion	Application Service		
SS02.tipo - plan	Application Service		
SS02.util - archivos	Application Service		
SS02.util - municipios	Application Service		
Servicio de Almacenamiento de Datos	Technology Service		
Servicio de Red	Technology Service		
Servicio de archivos	Technology Service		
Simulador	Application Component		
Simuladores	Application Service	Simuladores: Funcionalidades que permiten generar las simulaciones de los diferentes planes o modificaciones (incrementos y disminuciones) a los productos del Asociado.	

Nombre	Tipo	Documentación	Propiedad
Unidad de Solidaridad y Seguros	Grouping	La Unidad de Solidaridad y Seguros cuenta con un software integrado para su core de negocio denominado SIPAS (Sistema de Previsión, Asistencia y Solidaridad)	
Vinculación	Application Component		
app: Cotización y Ventas	Application Component		
app: Cotizador Web	Application Component	pkg: MiMutualWeb	
app: Implementación de Servicios	Application Component	Los componentes de este tipo se encargan de controlar y almacenar toda la lógica del negocio, validaciones y todo lo referente a procesamiento de datos.	
app: Mi Mutual Central	Application Component	Antes SIPAS, Mi Mutual es una aplicación web compuesta por distintos módulos de software con arreglo a todas las actividades necesarias que soportan la operación de los productos y servicios que ofrece la Unidad de Solidaridad y Seguros de la Cooperativa.	

Arq MiMutual. 4a1. Referencia

Mi Mutual. Coomeva, 2023.

Esquema de componentes Spring Boot

versión 0.1

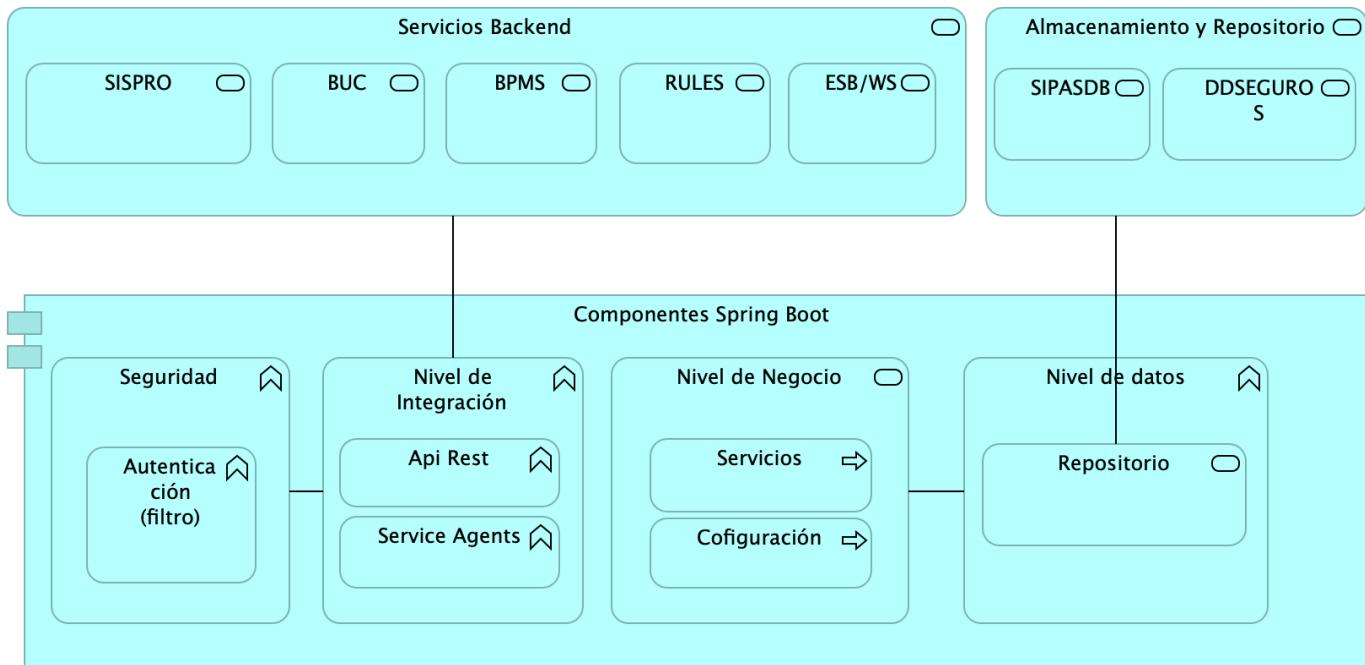
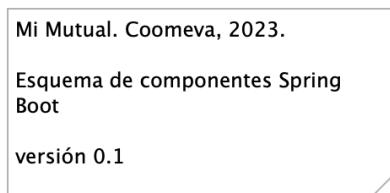


Imagen 5: Arq MiMutual. 4a1. Referencia

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 8: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
Almacenamiento y Repositorio	Application Service		
Api Rest	Application Function		
Autenticación (filtro)	Application Function		
BPMS	Application Service		
BUC	Application Service		
Cofiguración	Application Process		
Componentes Spring Boot	Application Component		
DDSEGUROS	Application Service		
ESB/WS	Application Service		
Nivel de Integración	Application Function		
Nivel de Negocio	Application Service		
Nivel de datos	Application Function		
RULES	Application Service		
Repositorio	Application Service		
SIPASDB	Application Service		
SISPRO	Application Service		
Seguridad	Application Function		
Service Agents	Application Function		
Servicios	Application Process		
Servicios Backend	Application Service		

Arq MiMutual. 4a3. Dependencias

Mi Mutual. Coomeva, 2023.

Mi Mutual Central. Paquetes: dependencias, roles, implementación funciones de aplicación.

versión 0.1

Paquetes y Dependencias Mi Mutual

La estructura está basada en spring boot y lenguaje de programación JAVA 8, conformada por componentes de aplicación y administración del ciclo de vida de los objetos.

Nombrado de paquetes para los servicios

- MiMutualWeb
- MiMutualProtecciones
- MiMutualReclamaciones
- MiMutualAsociados
- MiMutualUtilidades
- MiMutualBPM
- MiMutualReglas
- MiMutualIntegraciones
- MiMutualAuditoria
- MiMutualFlowable
- MiMutualSpringCloud

Entorno de Desarrollo

Para la etapa de desarrollo la aplicación estará configurada para levantar un servidor Tomcat embebido el cual se encuentra configurado el pom.xml y el cual permite trabajar de forma mucho más ágil.

Para el despliegue entre ambientes se manejará maven profiles con el fin de agregar las configuraciones de cada uno de estos.

El código fuente está alojado en un repositorio de Coomeva.

Mi Mutual. Coomeva, 2023.

Mi Mutual Central. Paquetes:
dependencias, roles, implementación
funciones de aplicación.

versión 0.1

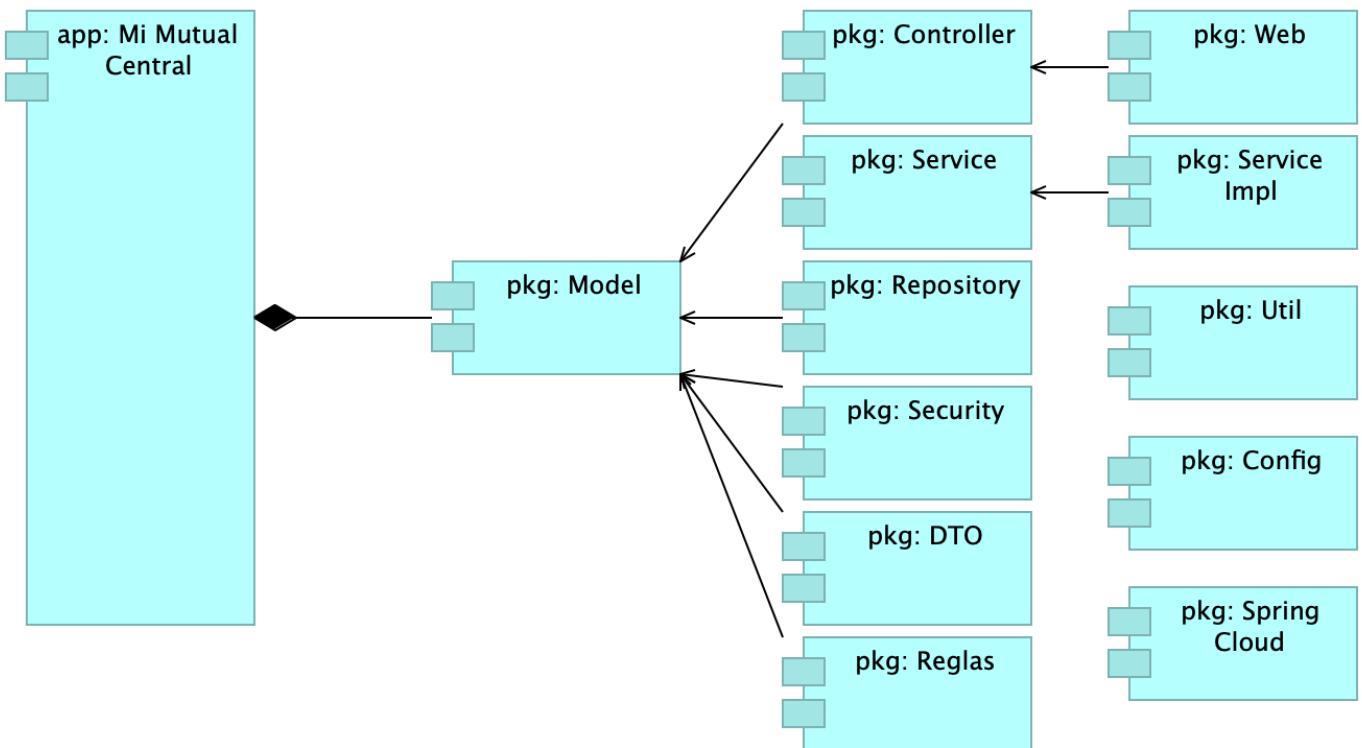


Imagen 6: Arq MiMutual. 4a3. Dependencias

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 9: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
app: Mi Mutual Central	Application Component	Antes SIPAS, Mi Mutual es una aplicación web compuesta por distintos módulos de software con arreglo a todas las actividades necesarias que soportan la operación de los productos y servicios que ofrece la Unidad de Solidaridad y Seguros de la Cooperativa.	
pkg: Config	Application Component	config: Almacenan todas las clases para la configuración del proyecto Spring.	
pkg: Controller	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: DTO	Application Component	dto: Almacenan todas las clases (pojos) para manejo de datos.	
pkg: Model	Application Component	model: Almacenan todas las clases (entities) que constituyen el modelo de datos.	

Nombre	Tipo	Documentación	Propiedad
pkg: Reglas	Application Component	dto: Almacenan todas las clases (pojos) para manejo de datos.	
pkg: Repository	Application Component	repository: Almacenan todas las interfaces y clases que constituyen el acceso a datos.	
pkg: Security	Application Component	security: Almacenan todas las clases que permiten la configuración de seguridad de la aplicación.	
pkg: Service	Application Component	service: Almacenan todas las interfaces que constituyen la lógica de negocio.	
pkg: Service Impl	Application Component	service.impl: Almacenan todas las clases que implementan la funcionalidad de las interfaces de service que constituyen la lógica de negocio.	
pkg: Spring Cloud	Application Component	dto: Almacenan todas las clases (pojos) para manejo de datos.	
pkg: Util	Application Component	util: Almacenan todas las clases de utilería para la aplicación.	
pkg: Web	Application Component	dto: Almacenan todas las clases (pojos) para manejo de datos.	

Arq MiMutual. 5. Físico (despliegue)

Mi Mutual. Coomeva, 2023.

Distribución física Mi Mutual. Estado actual, 2023.

versión 0.4.4

Especificaciones de despliegue Mi Mutual, 2023, componente central.

- Estándares para el manejo de servicios REST sobre HTTP 1.1
- Tecnologías para el backend: Java 8 con Spring Boot2.1.4
- Acceso a Datos: Spring Data 2.1.4
- Seguridad de las API: Spring Security + Oauth2.0
- Plataforma de despliegue Backend: Tomcat Spring boot
- Tecnologías para el frontend: Angular 12
- Librería de Estilos: Bootstrap 4
- Servidor web (HTTP 1.1): Apache 2.X

Mi Mutual. Coomeva, 2023.
 Distribución física Mi Mutual. Estado actual, 2023.
 versión 0.4.4

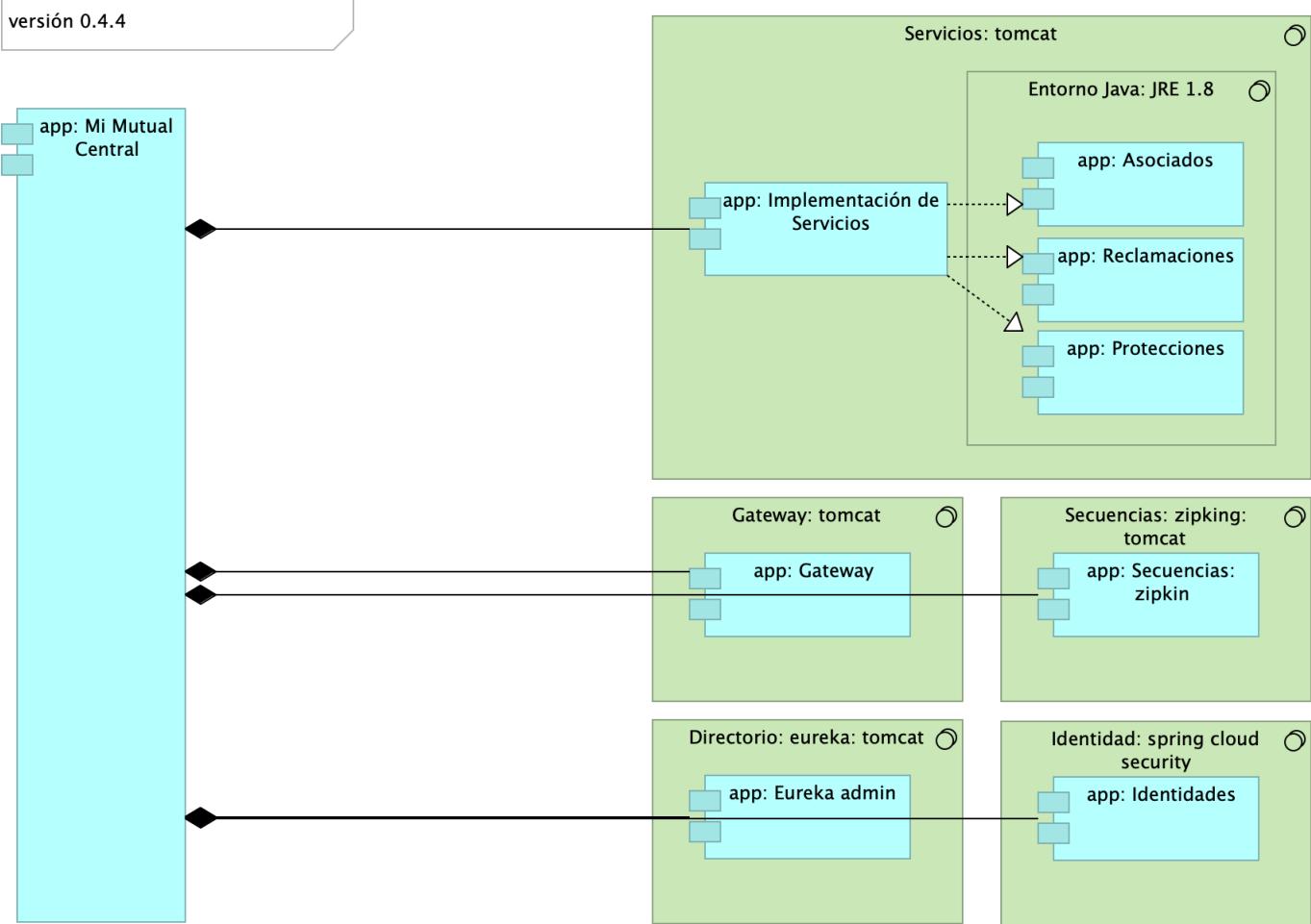


Imagen 7: Arq MiMutual. 5. Físico (despliegue)

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 10: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
Directorio: eureka: tomcat	System Software		
Entorno Java: JRE 1.8	System Software		
Gateway: tomcat	System Software		
Identidad: spring cloud security	System Software		
Secuencias: zipking: tomcat	System Software		
Servicios: tomcat	System Software		
app: Asociados	Application Component	Contiene todas las funcionalidades relacionadas con consulta y creación de asociados y beneficiarios.	
app: Eureka admin	Application Component	Contiene todas las funcionalidades relacionadas con registrar y localizar microservicios existentes, informar de su localización, su estado y datos relevantes de cada uno de ellos.	
app: Gateway	Application Component	Contiene todas las funcionalidades relacionadas con un proxy inverso que reenvía las llamadas relevantes a otros servicios.	

Nombre	Tipo	Documentación	Propiedad
app: Identidades	Application Component	Contiene todas las funcionalidades relacionadas con la gestión de los archivos de propiedades de los microservicios (Esta en construcción y no se ha integrado).	
app: Implementación de Servicios	Application Component	Los componentes de este tipo se encargan de controlar y almacenar toda la lógica del negocio, validaciones y todo lo referente a procesamiento de datos.	
app: Mi Mutual Central	Application Component	Antes SIPAS, Mi Mutual es una aplicación web compuesta por distintos módulos de software con arreglo a todas las actividades necesarias que soportan la operación de los productos y servicios que ofrece la Unidad de Solidaridad y Seguros de la Cooperativa.	
app: Protecciones	Application Component	Contiene todas las funcionalidades relacionadas con la gestión y configuración de productos y protecciones.	
app: Reclamaciones	Application Component	Contiene todas las funcionalidades relacionadas con la gestión de reclamaciones, liquidaciones y pagos.	
app: Secuencias: zipkin	Application Component	Contiene todas las funcionalidades relacionadas con la generación de IDs para la trazabilidad de los logs.	

Arq MiMutual. 6. Infraestructura

Mi Mutual. Coomeva, 2023.

Ambientes, Nodos (servidores), Elementos de red, Almacenamiento y equipos de hardware Mi Mutual. Estado Actual

versión 0.3

Mi Mutual. Coomeva, 2023.
 Ambientes, Nodos (servidores),
 Elementos de red, Almacenamiento y
 equipos de hardware Mi Mutual.
 Estado Actual
 versión 0.3

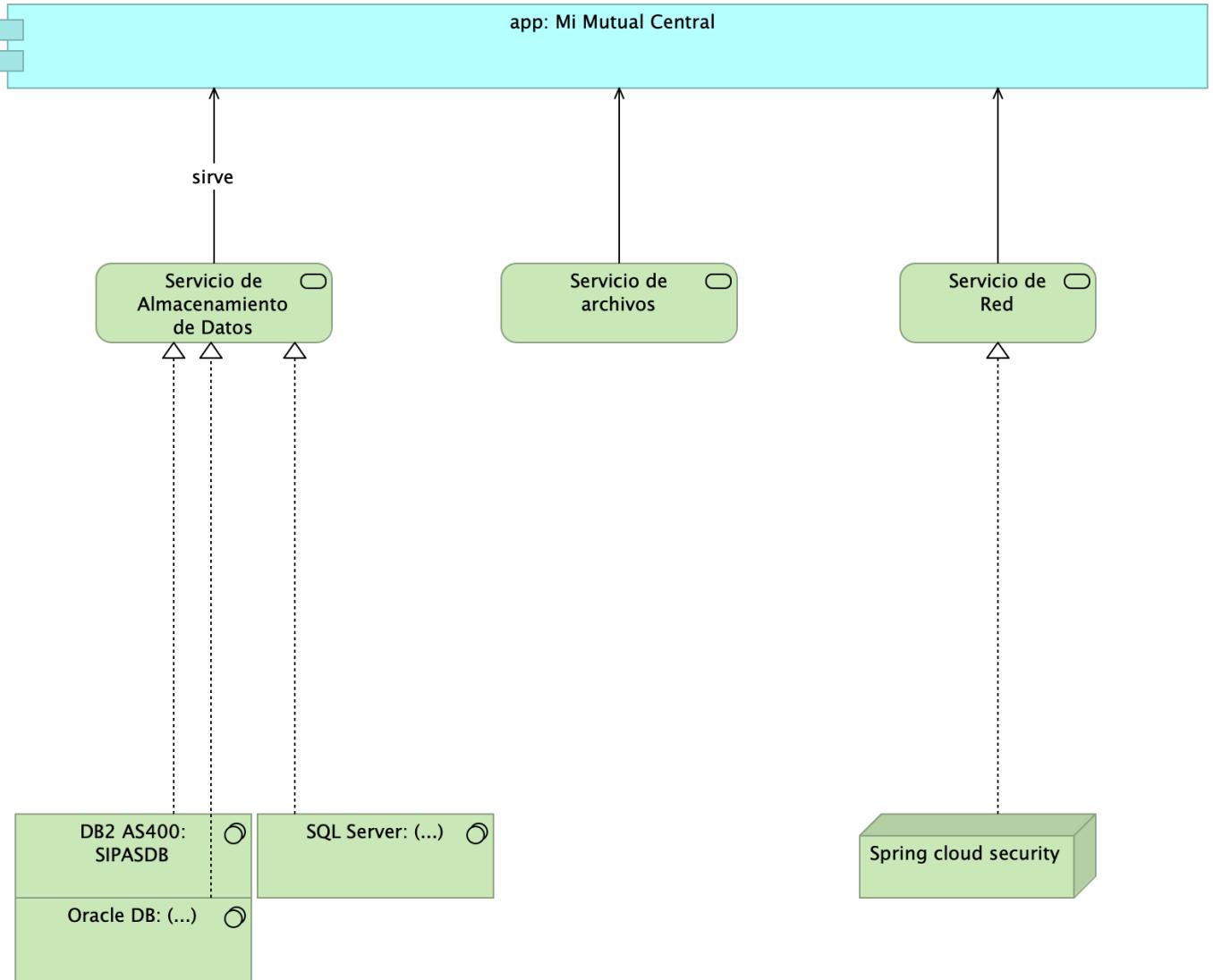


Imagen 8: Arq MiMutual. 6. Infraestructura

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Nombre	Tipo	Documentación	Propiedad
DB2 AS400: SIPASDB	System Software	Las bases de datos a utilizar son: * DB2 AS400: SIPASDB, * Sql Server (...), * Oracle (...)	
Oracle DB: (...)	System Software	Las bases de datos a utilizar son: * DB2 AS400: SIPASDB, * SQL Server (...), * Oracle (...)	
SQL Server: (...)	System Software	Las bases de datos a utilizar son: * DB2 AS400: SIPASDB, * SQL Server (...), * Oracle (...)	
Servicio de Almacenamiento de Datos	Technology Service		
Servicio de Red	Technology Service		
Servicio de archivos	Technology Service		

Nombre	Tipo	Documentación	Propiedad
Spring cloud security	Node	Se implementará Spring Boot Security y Spring Boot Oauth2 las cuales proveen una capa básica de seguridad entre Vista (Angular 2) y Controlador, obligando a que únicamente permita el acceso si se está autenticado si lo requiere, además para realizar el proceso de autenticación se utilizará la aplicación SISPRO (Coomeva) la cual funciona como un servidor de autenticación.	

La validación de roles se realizará a nivel de peticiones en el api rest según corresponda, siempre y cuando sea necesario, también se tendrán en cuenta otras validaciones como:

- Las credenciales que proporcionó no son válidas.
- El usuario está deshabilitado.
- Las credenciales de usuario han caducado.
- La cuenta de usuario ha caducado.
- La cuenta de usuario está bloqueada. | | app: Mi Mutual Central | Application Component | Antes SIPAS, Mi Mutual es una aplicación web compuesta por distintos módulos de software con arreglo a todas las actividades necesarias que soportan la operación de los productos y servicios que ofrece la Unidad de Solidaridad y Seguros de la Cooperativa. | |

Table: Elementos de la vista. {#tbl:tblElement-ArqMiMutual.6.Infraestructura-id}

Arq MiMutual. 7. Datos. Negocio

Mi Mutual. Coomeva, 2023.

Mi Mutual Central. Entidades: Estructuras, objeto, relaciones con aplicación.

versión 0.1

Entidades de Negocio Mi Mutual

Dominios de datos de negocio. Entidades independiente de la plataforma y de la tecnología.

- Configuración (caracterización de productos, plan)
- Plan (producto pólizas seguros)
- Canal (medios del tomador/asociado)
- Parámetros globales (catálogos)
- Portafolio de asociado
- Asociado
- Facturación
- Beneficiario

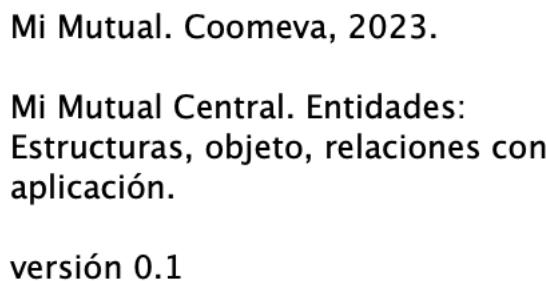


Imagen 9: Arq MiMutual. 7. Datos. Negocio

Fuente: *Repositorio arquitectura Mi Mutual (2023)*

Catálogo de Elementos

Tabla 11: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
DAT00.Asociado	Business Object		
DAT00.Beneficiario	Business Object		
DAT00.Canal (medios del tomador/asociado)	Business Object		
DAT00.Configuración (caracterización)	Business Object	Caracterización de productos, planes, parámetros	
DAT00.Facturación	Business Object		
DAT00.Parametros globales (catálogos)	Business Object		
DAT00.Plan (producto pólizas seguros)	Business Object		
DAT00.Portafolios de asociados	Business Object		

Arq MiMutual. 7a. Datos. Aplicación

Mi Mutual. Coomeva, 2023.

Mi Mutual Central. Físico. Entidades: Estructuras, objeto, relaciones con entidades.

versión 0.1

Estructuras de datos específicas a la plataforma. Modelo de negocio para las aplicaciones.

Modelo físico facilitadas por Coomeva, corte del 2 de mayo de 2022. Contiene las estructuras de configuración de fondo, cliente, planes, cobertura y planes de coberturas.

Mi Mutual. Coomeva, 2023.
 Mi Mutual Central. Físico. Entidades:
 Estructuras, objeto, relaciones con
 entidades.
 versión 0.1



Imagen 10: Arq MiMutual. 7a. Datos. Aplicación

Fuente: *Repositorio arquitectura Mi Mutual (2023)*

Catálogo de Elementos

Tabla 12: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
DAT01.ADICIONAL PLAN COBERTURA	Data Object		
DAT01.ASISTENCIA PLAN COBERTURA	Data Object		
DAT01.ASISTENCIA PLAN COBERTURA DETALLE	Data Object		
DAT01.BENEFICIARIO ASISTENCIA	Data Object		
DAT01.BENEFICIO PREEXISTENCIA	Data Object		
DAT01.CAMPANA RELACION PLAN COBERTURA	Data Object		
DAT01.CANAL	Data Object		
DAT01.CANAL EVENTO	Data Object		

Nombre	Tipo	Documentación	Propiedad
DAT01.CANAL VENTA EXCLUSION	Data Object		
DAT01.CANAL VENTA EXCLUSION COBERTURA	Data Object		
DAT01.CICLO FACTURACION CONFIG MOV	Data Object		
DAT01.CLIENTE	Data Object		
DAT01.COBERTURA	Data Object		
DAT01.COBERTURA BENEFICIARIO COBERTURA	Data Object		
DAT01.COBERTURA BENEFICIARIO PAGO	Data Object		
DAT01CONDICION PAGO ANTIGUEDAD	Data Object		
DAT01CONDICION PAGO EVENTO	Data Object		
DAT01CONDICION PLAN	Data Object		
DAT01CONDICION VENTA	Data Object		
DAT01CONDICIONES	Data Object		
DAT01CONFIGURACION DIAGNOSTICOS	Data Object		
DAT01CONFIGURACION MOV DETALLE	Data Object		
DAT01CONFIGURACION MOVIMIENTO	Data Object		
DAT01CONTROL ARE TECNICA	Data Object		
DAT01CONTROL CUMULO	Data Object		
DAT01CUMULO	Data Object		
DAT01CUMULOS COBERTURA	Data Object		
DAT01CUMULOS PLAN COBERTURA	Data Object		
DAT01DEDUCIBLE	Data Object		
DAT01DESMEMBRACION ACCIDENTE	Data Object		
DAT01DESMEMBRACION ACCIDENTE PLAN COBERTURA	Data Object		
DAT01DOCUMENTO REQUISITO	Data Object		
DAT01DOCUMENTOS SOLICITUD EVENTO	Data Object		
DAT01ENFERMEDAD GRAVE	Data Object		
DAT01ENFERMEDAD GRAVE PLAN COBERTURA	Data Object		
DAT01ESTADO ASOCIADO	Data Object		
DAT01EVENTO COBERTURA	Data Object		
DAT01EXCLUSION	Data Object		
DAT01EXCLUSION COBERTURA	Data Object		
DAT01EXCLUSION PLAN COBERTURA	Data Object		
DAT01EXCLUSION PLAN COBERTURA DETALLE	Data Object		
DAT01FAC CONCEPTO PLAN	Data Object		
DAT01FONDO	Data Object		
DAT01FORMULA PLAN	Data Object		
DAT01GENERO REQUISITO	Data Object		
DAT01LIQUIDACION	Data Object		
DAT01LIQUIDACION DETALLE	Data Object		
DAT01NIVEL RIESGO COBERTURA	Data Object		
DAT01NIVEL RIESGO CONFIG MOV	Data Object		
DAT01NIVELES NOTAS PLAN COBERTURA	Data Object		
DAT01NOTA ACLARATORIA PLAN	Data Object		
DAT01NOTIFICACION EVENTO	Data Object		
DAT01ORIGEN COBERTURA COBERTURA	Data Object		
DAT01PERIODO CARENCIA	Data Object		
DAT01PERSONA	Data Object		
DAT01PLAN	Data Object		
DAT01PLAN CANAL VENTA	Data Object		
DAT01PLAN COBERTURA	Data Object		
DAT01PLAN COBERTURA DEPENDIENTE	Data Object		
DAT01PLAN COBERTURA EDAD	Data Object		
DAT01PLAN COBERTURA REQUISITO	Data Object		
DAT01PLAN FRECUENCIA FACTURACION	Data Object		
DAT01PLAN MEDIO FACTURACION	Data Object		

Nombre	Tipo	Documentación	Propiedad
DAT01.PLAN NIVEL RIESGO	Data Object		
DAT01.PLAN OBLIGATORIO	Data Object		
DAT01.PLAN PARENTESCO	Data Object		
DAT01.PLAN PERSEVERANTE	Data Object		
DAT01.PORCENTAJE CUOTA	Data Object		
DAT01.PRODUCTO COBERTURA	Data Object		
DAT01.PRODUCTO EXCLUSIVO	Data Object		
DAT01.PROMOCION CANAL	Data Object		
DAT01.PROMOCION CONDICION	Data Object		
DAT01.PROMOCION PLAN COBERTURA	Data Object		
DAT01.PROMOTOR CANAL	Data Object		
DAT01.RECONOCIMIENTO POR PERMANENCIA	Data Object		
DAT01.REGLAS EXCEPCIONES	Data Object		
DAT01.REQUISITO CONTROL MEDICO	Data Object		
DAT01.RESPONSABLE PERSONA	Data Object		
DAT01.SOLICITUD EVENT	Data Object		
DAT01.SOLICITUD EVENTO DETALLE	Data Object		
DAT01.SUBLIMITE COBERTURA	Data Object		
DAT01.SUBSISTENTE PLAN COBERTURA	Data Object		
DAT01.SUBSISTENTE PLAN COBERTURA DETALLE	Data Object		
DAT01.TIPO MOVIMIENTO	Data Object		
DAT01.TIPO PROCESO CUMULO	Data Object		
DAT01.TRANSACCION EXCLUSION	Data Object		
DAT01.TRANSACCION EXCLUSION COBERTURA	Data Object		
DAT01.TRANSACCION REQUISITO	Data Object		
DAT01.VALOR ASEGURADO	Data Object		
DAT01.VALOR ASEGURADO PLAN COBERTURA	Data Object		
DAT01.VALOR ASEGURADO TOPE	Data Object		
DAT01.VALOR CUOTA PLAN COBERTURA	Data Object		
DAT01.VALOR RESCATE	Data Object		

Arq MiMutual. 7b. Datos. Relaciones

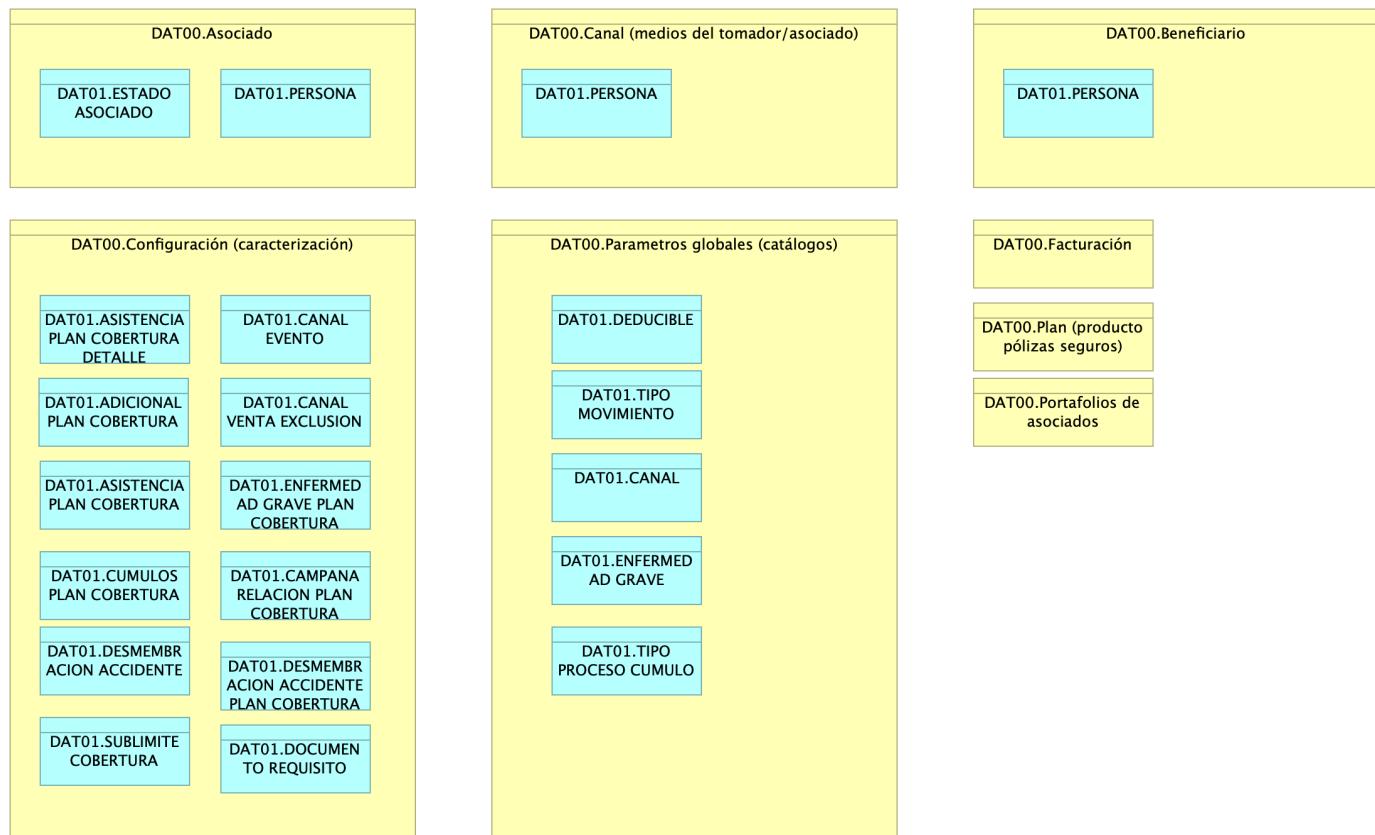
Mi Mutual. Coomeva, 2023.

Mi Mutual Central. Entidades: Estructuras, objeto, relaciones con aplicación.

versión 0.2.3

Entidades de Negocio Mi Mutual

- Configuración (caracterización de productos, plan)
- Plan (producto pólizas seguros)
- Canal (medios del tomador/asociado)
- Parámetros globales (catálogos)
- Portafolio de asociado
- Asociado
- Facturación
- Beneficiario

**Imagen 11:** Arq MiMutual. 7b. Datos. RelacionesFuente: *Repositorio arquitectura Mi Mutual (2023)*

Catálogo de Elementos

Tabla 13: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
DAT00.A sociado	Business Object		
DAT00.Beneficiario	Business Object		
DAT00.Canal (medios del tomador/asociado)	Business Object		
DAT00.Configuración (caracterización)	Business Object	Caracterización de productos, planes, parámetros	
DAT00.Facturación	Business Object		
DAT00.Parametros globales (catálogos)	Business Object		
DAT00.Plan (producto pólizas seguros)	Business Object		
DAT00.Portafolios de asociados	Business Object		
DAT01.ADJACIONAL PLAN COBERTURA	Data Object		
DAT01.ASISTENCIA PLAN COBERTURA	Data Object		
DAT01.ASISTENCIA PLAN COBERTURA DETALLE	Data Object		
DAT01.CAMPANA RELACION PLAN COBERTURA	Data Object		
DAT01.CANAL	Data Object		
DAT01.CANAL EVENTO	Data Object		
DAT01.CANAL VENTA EXCLUSION	Data Object		
DAT01.CUMULOS PLAN COBERTURA	Data Object		
DAT01.DEDUCIBLE	Data Object		
DAT01.DESMEMBRACION ACCIDENTE	Data Object		
DAT01.SUBLIMITE COBERTURA	Data Object		
DAT01.DOCUMENTO REQUISITO	Data Object		

Nombre	Tipo	Documentación	Propiedad
DAT01.DESMEMBRACION ACCIDENTE PLAN COBERTURA	Data Object		
DAT01.DOCUMENTO REQUISITO	Data Object		
DAT01.ENFERMEDAD GRAVE	Data Object		
DAT01.ENFERMEDAD GRAVE PLAN COBERTURA	Data Object		
DAT01.ESTADO ASOCIADO	Data Object		
DAT01.PERSONA	Data Object		
DAT01.SUBLIMITE COBERTURA	Data Object		
DAT01.TIPO MOVIMIENTO	Data Object		
DAT01.TIPO PROCESO CUMULO	Data Object		

ArqCotizador. 1. Contexto

Mi Mutual. Coomeva, 2023.

Cotizador Web Mi Mutual. Contexto Mi Mutual: Áreas negocio, componente central Mi Mutual, servicios y funciones.

versión 0.1

Contexto Mi Mutual Web

La aplicación Cotizador Web hace parte de los módulos de interfaz web de Mi Mutual Central, representado por API Mi Mutual en el diagrama. Realizar cotizaciones de los planes de protección luego de la vinculación del asociado.

La estructura por módulos permite realizar aplicaciones escalables y robustas ya que permite organizar las partes de la aplicación, la organización en bloques, extender la aplicación con funcionalidades de librerías externas, proporcionar un entorno de resolución de plantillas y además permite especificar la forma de la carga de cada uno de los componentes y servicios que conforman un módulo.

Módulos Externos

Los módulos externos son todas y cada uno de las herramientas que se utilizan para complementar con funcionalidades ya desarrolladas y tomadas desde un repositorio externo (NPM).

- TranslateModule: Manejo de internacionalización. Documentación: <https://github.com/ngx-translate/core>
- NgxMaskModule: Manejo de máscaras de input text. Documentación: <https://github.com/JsDaddy/ngx-mask>
- JwtModule: Manejo de token. Documentación: <https://github.com/auth0/angular2-jwt>
- sweetalert2: Manejo de alertas de mensajes. Documentación: <https://sweetalert2.github.io/>
- ngx-ui-loader: Manejo de Spinner para control de peticiones asíncronas. Documentación: <https://github.com/t-ho/ngx-ui-loader>
- Ngprime: Manejo de componentes visuales Documentación: <https://www.primefaces.org/primeng/#/>
- chart.js: componente utilizado para el manejo de graficas Documentación: <https://www.chartjs.org/docs/latest/>
- classlist.js: componente para el manejo de listas de datos en las gráficas Documentación: <https://www.chartjs.org/docs/latest/>
- cronstrue: componente para traducir una expresión cron a palabras Documentación: <https://github.com;bradymholt/cronstrue>
- file-saver: componente para descargar un archivo desde los bytes Documentación: <https://github.com/eligrey/FileSaver.js#readme>
- ngx-tinymce: Editor html para generación de plantillas para cartas Documentación: <https://cipchk.github.io/ngx-tinymce/#/>
- quill: componente para editor html Documentación: <https://quilljs.com/>

Servicios Transversales

- AuthGuard: Validación de existencia de autenticación
- DeactiveGuard: Validación de salida de un componente
- ErrorInterceptor: Interceptor de Errores del back
- JwtInterceptor: Interceptor para injectar el token
- AuthenticationService: Métodos para completar la autenticación
- TypesService: Consumo de servicios de parametrización
- IdleTimeoutService: Verificación de timeout del token

Mi Mutual. Coomeva, 2023.
 Cotizador Web Mi Mutual. Contexto
 Mi Mutual: Áreas negocio,
 componente central Mi Mutual,
 servicios y funciones.
 versión 0.1

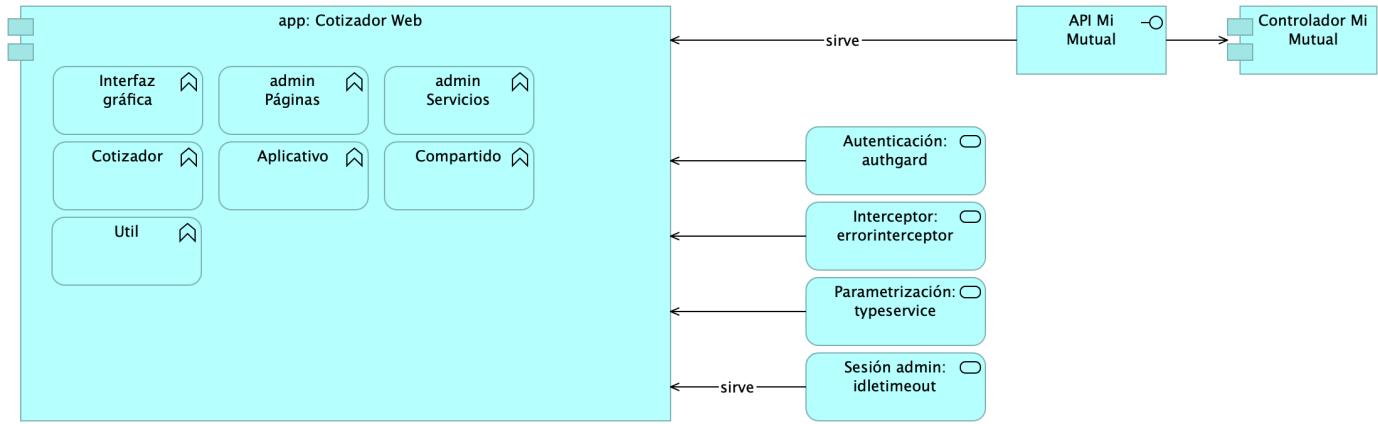


Imagen 12: ArqCotizador. 1. Contexto

Fuente: *Repositorio arquitectura Mi Mutual (2023)*

Catálogo de Elementos

Tabla 14: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
API Mi Mutual	Application Interface		
Aplicativo	Application Function		
Autenticación: authgard	Application Service		
Compartido	Application Function		
Controlador Mi Mutual	Application Component	Los componentes de este tipo se encargan de controlar los servicios rest de la aplicación, además en estos componentes se define la forma como se reciben y envían los datos de los servicios rest y la seguridad de cada uno de los métodos.	
Cotizador	Application Function		
Interceptor: errorinterceptor	Application Service		
Interfaz gráfica	Application Function		
Parametrización: typeservice	Application Service		
Sesión admin: idletimeout	Application Service		
Util	Application Function	En la Utilidades se especifican las clases que complementan una funcionalidad de un componente o servicio. * FormValidate: Clase que implementa un disparador de validación de todos los campos de un formulario. * CustomValidators: Creación de validaciones de campos.	
admin Páginas	Application Function		
admin Servicios	Application Function		
app: Cotizador Web	Application Component	pkg: MiMutualWeb	

ArqCotizador. 2. Contenedores

Mi Mutual. Coomeva, 2023.

Estructura de componentes principales, Cotizador Web, Mi Mutual. Roles de componentes, separación responsabilidades.

versión 0.2

Mi Mutual. Coomeva, 2023.
Estructura de componentes principales, Cotizador Web, Mi Mutual. Roles de componentes, separación responsabilidades.
versión 0.2

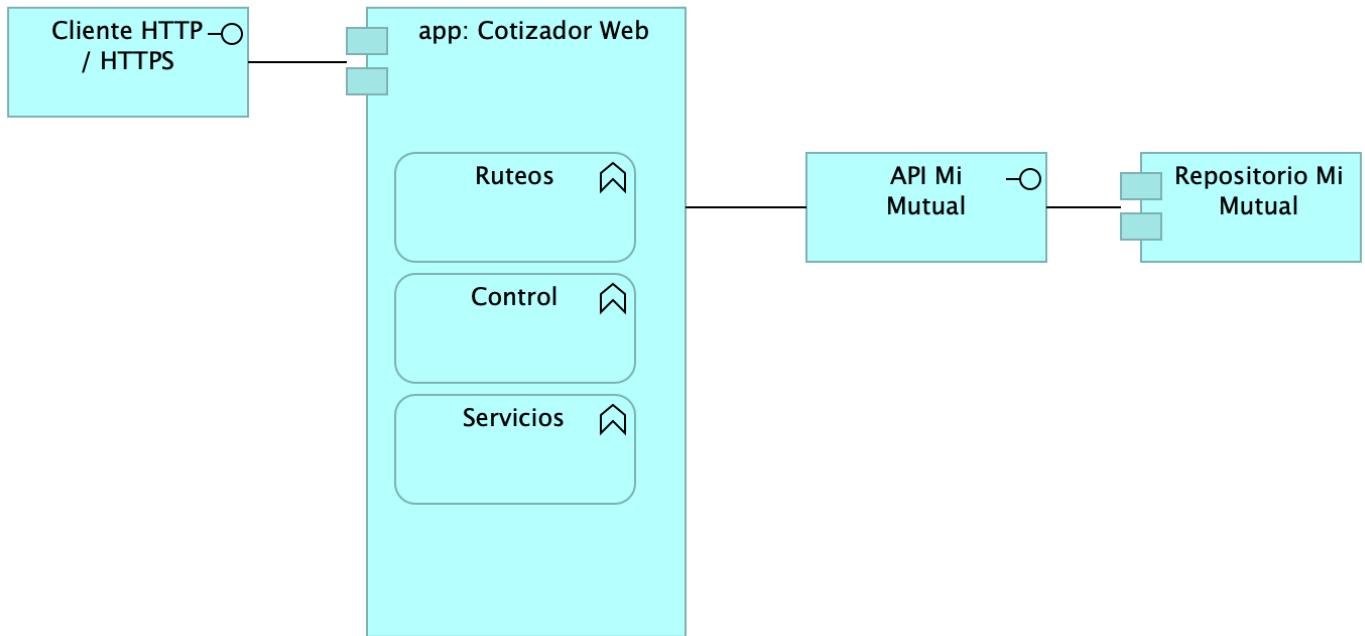


Imagen 13: ArqCotizador. 2. Contenedores

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 15: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
API Mi Mutual	Application Interface		
Cliente HTTP / HTTPS	Application Interface		
Control	Application Function		

Nombre	Tipo	Documentación	Propiedad
Repositorio Mi Mutual	Application Component	<p>Antes SIPAS, Mi Mutual es una aplicación web compuesta por distintos módulos de software con arreglo a todas las actividades necesarias que soportan la operación de los productos y servicios que ofrece la Unidad de Solidaridad y Seguros de la Cooperativa.</p> <p>Para el manejo de la persistencia de datos se utilizará Spring Data el cual se apoya en la especificación de JPA y en la implementación de HIBERNATE además de complementar esta capa de persistencia con nuevas funcionalidades que facilitan el acceso a datos.</p>	
Ruteos	Application Function		
Servicios	Application Function		
app: Cotizador Web	Application Component	pkg: MiMutualWeb	

ArqCotizador. 4. Aplicación

Mi Mutual. Coomeva, 2023.

Organización de aplicación Cotizador Web, Mi Mutual. Estado Actual. Segmentos (1) frontal, (2) servicios, (3) central/negocio Mi Mutual, (4) infraestructura.

versión 0.4.1

La organización de la aplicación Cotizador Web Mi Mutual, como capa de presentación y servicios, plantea una estructura basada en la referencia de aplicaciones Angular 12. Las características de esta estructura (referida por Angular) está orientada al crecimiento (tamaño) de la aplicación, la escalabilidad y al rendimiento. La aplicación web Cotizador está diseñada (modulos) para manejar la carga por demanda del contenido.

Mi Mutual. Coomeva, 2023.
 Organización de aplicación Cotizador Web, Mi Mutual. Estado Actual.
 Segmentos (1) frontal, (2) servicios, (3) central/negocio Mi Mutual, (4) infraestructura.
 versión 0.4.1

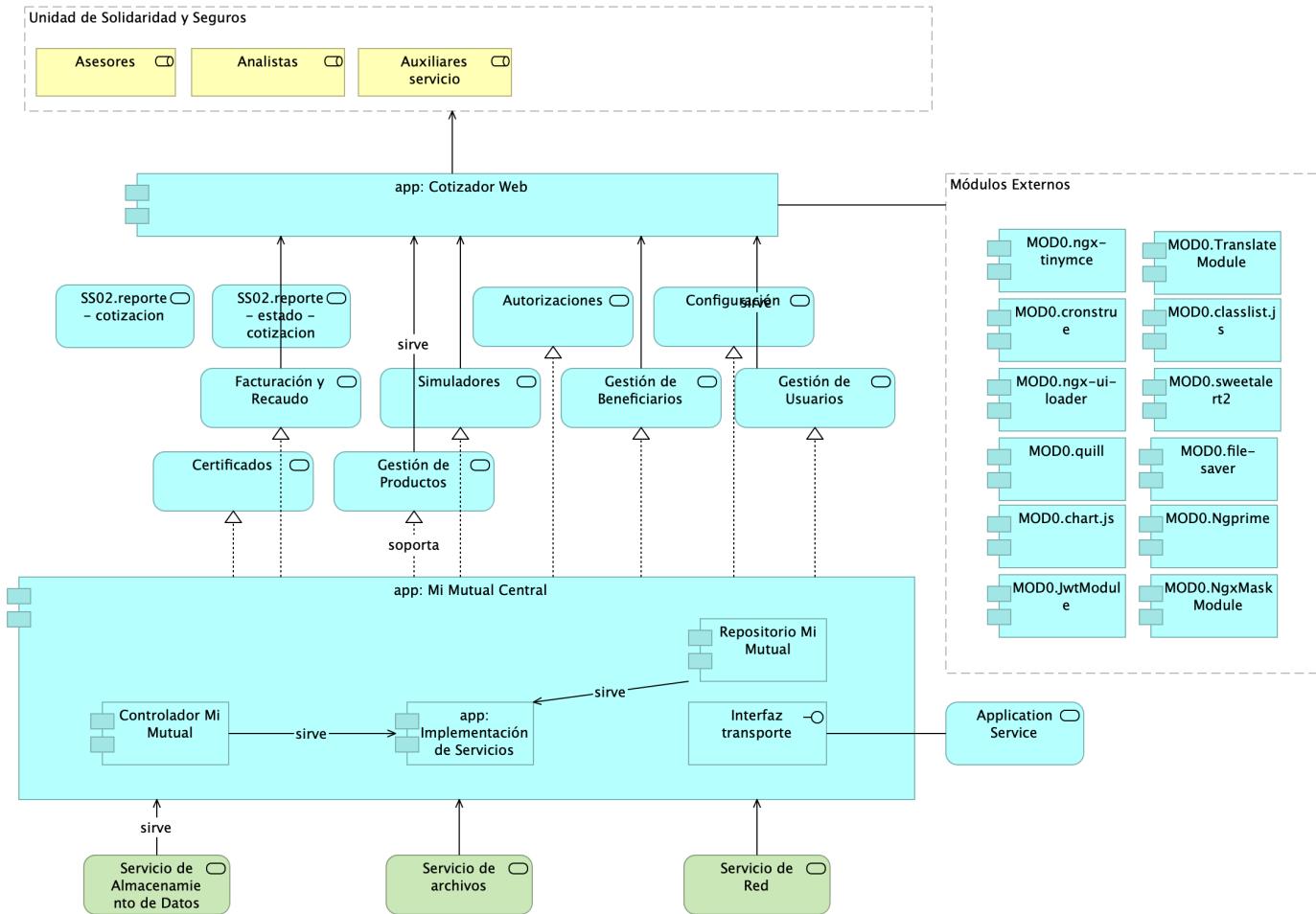


Imagen 14: ArqCotizador. 4. Aplicación

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 16: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
Analistas	Business Role	Analistas y auxiliares de servicio regional y nacional, agentes del centro de contacto, auditores médicos, analistas de operaciones (aseguramiento y facturación) y jefes.	
Application Service	Application Service	Otros servicios del contexto de Mi Mutual Central.	
Asesores	Business Role	Asesores integrales	
Autorizaciones	Application Service	Autorizaciones: Administración de peticiones de autorización y sus correspondientes aprobaciones usando el servicio del flujo de procesos.	

Nombre	Tipo	Documentación	Propiedad
Auxiliares servicio	Business Role	Analistas y auxiliares de servicio regional y nacional, agentes del centro de contacto, auditores médicos, analistas de operaciones (aseguramiento y facturación) y jefes.	
Certificados	Application Service	Certificados: Permite la generación de los certificados de valores de protección y contribuciones pagadas, de retención en la fuente, de pagos de perseverancia y de cobertura de auxilio funerario.	
Configuración	Application Service	Configuración o parametrización de factores para realizar los cálculos de las contribuciones de los asociados a la Cooperativa para cada uno de los productos adquiridos.	
Controlador Mi Mutual	Application Component	Los componentes de este tipo se encargan de controlar los servicios rest de la aplicación, además en estos componentes se define la forma como se reciben y envían los datos de los servicios rest y la seguridad de cada uno de los métodos.	
Facturación y Recaudo	Application Service	Administración de la facturación y recaudo diario de los productos	
Gestión de Beneficiarios	Application Service	Gestión de Beneficiarios: Permite administrar la información relacionada con los beneficiarios del Asociado, permitiendo ejecutar operaciones de consulta, inserción y modificación	
Gestión de Productos	Application Service	Gestión de productos del fondo mutual y auxilio funerario que involucran lo relacionado a las siguientes coberturas: * Fondo de Solidaridad: Incapacidades temporales, Incapacidades Permanentes (total, parcial), Perseverancia 60, 62, 65, 70 años, Perseverancias Anticipadas, Fallecimiento Asociado (Auxilio por muerte), Desempleo, Disminución de ingresos y enfermedades graves; Rentas por hospitalización, Enfermedades de Alto Costo, Pólizas de seguros personales y patrimoniales, Planes educativos, Segunda opinión médica, Asistencias. * Auxilio Funerario: Fallecimiento de familiares directos (inscritos) del Asociado.	
Gestión de Usuarios	Application Service	Gestión de Usuarios: Administración de la información relacionada con los usuarios del sistema. Este componente se comunica con el servicio unificado de autenticación y autorización que devuelve los permisos que un usuario posee sobre las opciones que proporciona el sistema.	
Interfaz transporte	Application Interface	Feign Client. Integración con otros sistemas para facilitar los procesos de vinculación, retiro, reactivación o fallecimiento de asociados.	

Nombre	Tipo	Documentación	Propiedad
MOD0.JwtModule	Application Component	Manejo de token. Documentación: https://github.com/auth0/angular2-jwt	
MOD0.Ngprime	Application Component	Manejo de componentes visuales Documentación: https://www.primefaces.org/primeng/#/	
MOD0.NgxMaskModule	Application Component	Manejo de máscaras de input text. Documentación: https://github.com/JsDaddy/ngx-mask	
MOD0.TranslateModule	Application Component	Manejo de internacionalización. Documentación: https://github.com/ngx-translate/core	
MOD0.chart.js	Application Component	Componente utilizado para el manejo de graficas Documentación: https://www.chartjs.org/docs/latest/	
MOD0.classList.js	Application Component	Componete para el manejo de listas de datos en las gráficas Documentación: https://www.chartjs.org/docs/latest/	
MOD0.crontrue	Application Component	Componente para traducir una expresión cron a palabras Documentación: https://github.com;bradymholt/crontrue	
MOD0.file-saver	Application Component	Componente para descargar un archivo desde los bytes Documentación: https://github.com/eligrey/FileSaver.js#readme	
MOD0.ngx-tinymce	Application Component	Editor html para generación de plantillas para cartas Documentación: https://cipchk.github.io/ngx-tinymce/#/	
MOD0.ngx-ui-loader	Application Component	Manejo de Spinner para control de peticiones asíncronas. Documentación: https://github.com/t-ho/ngx-ui-loader	
MOD0.quill	Application Component	Cponente para editor html Documentación: https://quilljs.com/	
MOD0/sweetalert2	Application Component	Manejo de alertas de mensajes. Documentación: https://sweetalert2.github.io/	
Módulos Externos	Grouping		
Repositorio Mi Mutual	Application Component	Antes SIPAS, Mi Mutual es una aplicación web compuesta por distintos módulos de software con arreglo a todas las actividades necesarias que soportan la operación de los productos y servicios que ofrece la Unidad de Solidaridad y Seguros de la Cooperativa. Para el manejo de la persistencia de datos se utilizará Spring Data el cual se apoya en la especificación de JPA y en la implementación de HIBERNATE además de complementar esta capa de persistencia con nuevas funcionalidades que facilitan el acceso a datos.	
SS02.reporte - cotizacion	Application Service		
SS02.reporte - estado - cotizacion	Application Service		
Servicio de Almacenamiento de Datos	Technology Service		
Servicio de Red	Technology Service		

Nombre	Tipo	Documentación	Propiedad
Servicio de archivos	Technology Service		
Simuladores	Application Service	Simuladores: Funcionalidades que permiten generar las simulaciones de los diferentes planes o modificaciones (incrementos y disminuciones) a los productos del Asociado.	
Unidad de Solidaridad y Seguros	Grouping	La Unidad de Solidaridad y Seguros cuenta con un software integrado para su core de negocio denominado SIPAS (Sistema de Previsión, Asistencia y Solidaridad)	
app: Cotizador Web	Application Component	pkg: MiMutualWeb	
app: Implementación de Servicios	Application Component	Los componentes de este tipo se encargan de controlar y almacenar toda la lógica del negocio, validaciones y todo lo referente a procesamiento de datos.	
app: Mi Mutual Central	Application Component	Antes SIPAS, Mi Mutual es una aplicación web compuesta por distintos módulos de software con arreglo a todas las actividades necesarias que soportan la operación de los productos y servicios que ofrece la Unidad de Solidaridad y Seguros de la Cooperativa.	

ArqCotizador. 4a. Aplicación. Servicios

Mi Mutual. Coomeva, 2023.

Especificaciones de Servicios. Aplicación Cotizador Web, Mi Mutual. Estado Actual. Estructura interna, comunicación e interfaces.

versión 0.1

Composición interna de los servicios de Mi Mutual Central, Mi Mutual Web, Cotizador Web.

Mi Mutual. Coomeva, 2023.

Especificaciones de Servicios.
Aplicación Cotizador Web, Mi Mutual.
Estado Actual. Estructura interna,
comunicación e interfaces.

versión 0.1

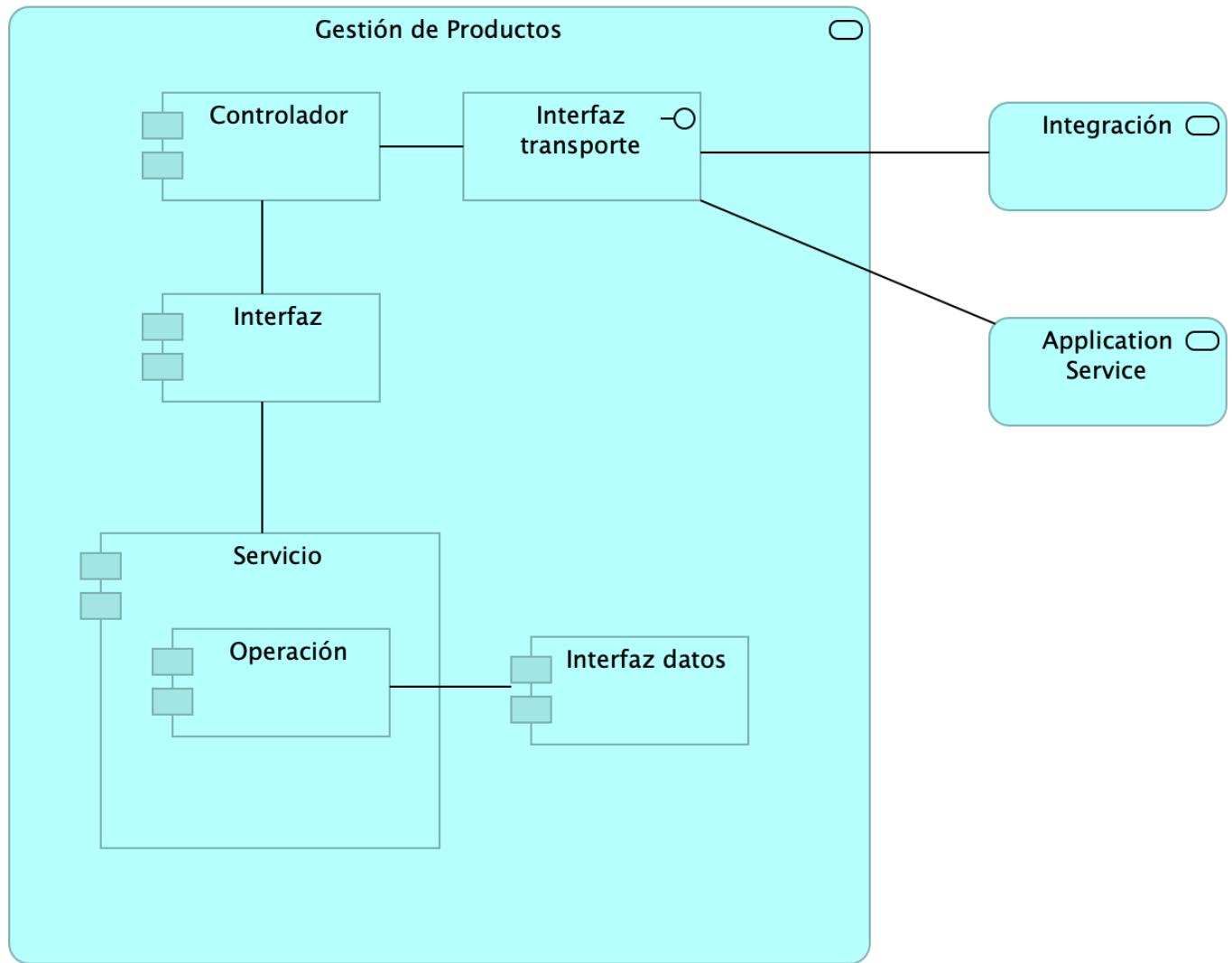


Imagen 15: ArqCotizador. 4a. Aplicación. Servicios

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 17: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
Application Service	Application Service	Otros servicios del contexto de Mi Mutual Central.	
Controlador	Application Component	Controlador interno del servicio. Punto de entrada a la lógica de expuesta.	

Nombre	Tipo	Documentación	Propiedad
Gestión de Productos	Application Service	Gestión de productos del fondo mutual y auxilio funerario que involucran lo relacionado a las siguientes coberturas: * Fondo de Solidaridad: Incapacidades temporales, Incapacidades Permanentes (total, parcial), Perseverancia 60, 62, 65, 70 años, Perseverancias Anticipadas, Fallecimiento Asociado (Auxilio por muerte), Desempleo, Disminución de ingresos y enfermedades graves; Rentas por hospitalización, Enfermedades de Alto Costo, Pólizas de seguros personales y patrimoniales, Planes educativos, Segunda opinión médica, Asistencias. * Auxilio Funerario: Fallecimiento de familiares directos (inscritos) del Asociado.	
Integración	Application Service		
Interfaz	Application Component	Interfaz de inversión de dependencia a las clases del servicio.	
Interfaz datos	Application Component	Acceso a datos del modelo del contexto de Mi Mutual Central.	
Interfaz transporte	Application Interface	Feign Client. Integración con otros sistemas para facilitar los procesos de vinculación, retiro, reactivación o fallecimiento de asociados.	
Operación	Application Component		
Servicio	Application Component	Exposición de componentes de negocio.	

ArqCotizador. 4a. Dependencias

Mi Mutual. Coomeva, 2023.

Mi Mutual Web. Paquetes: dependencias, roles, implementación funciones de aplicación.

versión 0.1

Paquetes y Dependencias Cotizador Web

Módulos y componentes que hacen parte de la estructura de la aplicación Cotizador Web (basado en Angular 12 ¹).

Módulos Cotizador Web

La estructura por módulos actual apunta a la escalabilidad y mantenimiento del Cotizador en términos de: organizar las partes de la aplicación, organización los bloques, extender la aplicación con librerías externas, proporcionar un entorno de resolución de plantillas y además, distribuir las cargas de los componentes y servicios que usa la aplicación.

Mi Mutual. Coomeva, 2023.
 Mi Mutual Web. Paquetes:
 dependencias, roles, implementación
 funciones de aplicación.
 versión 0.1

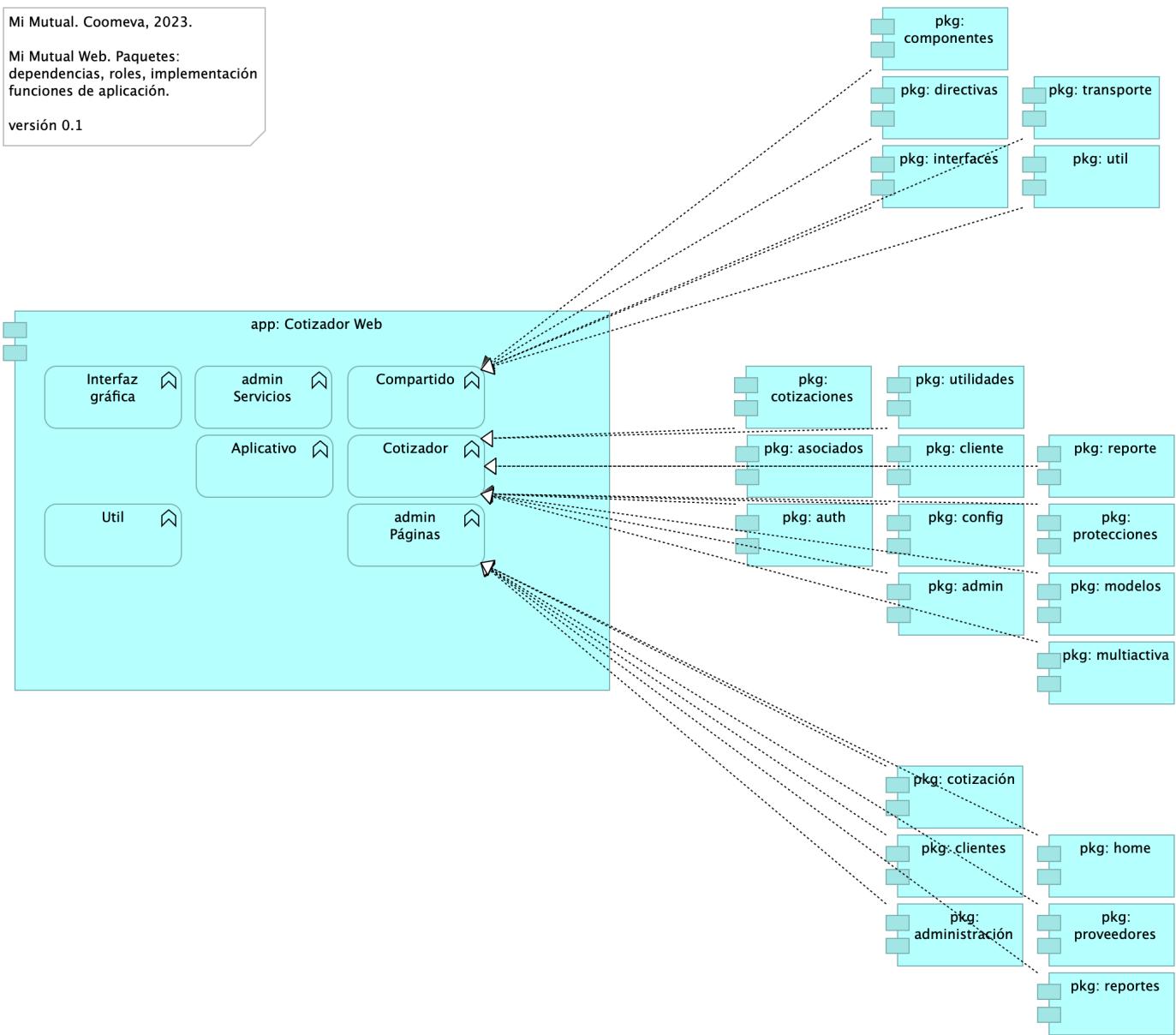


Imagen 16: ArqCotizador. 4a. Dependencias

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 18: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
Aplicativo	Application Function		
Compartido	Application Function		
Cotizador	Application Function		
Interfaz gráfica	Application Function		
Util	Application Function	<p>En la Utilidades se especifican las clases que complementan una funcionalidad de un componente o servicio.</p> <p>* FormValidate: Clase que implementa un disparador de validación de todos los campos de un formulario.</p> <p>* CustomValidators: Creación de validaciones de campos.</p>	

Nombre	Tipo	Documentación	Propiedad
admin Páginas	Application Function		
admin Servicios	Application Function		
app: Cotizador Web	Application Component	pkg: MiMutualWeb	
pkg: admin	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: administración	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: asociados	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: auth	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: cliente	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: clientes	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: componentes	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: config	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: cotizaciones	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: cotización	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: directivas	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: home	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: interfaces	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: modelos	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: multiactiva	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: protecciones	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: proveedores	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: reporte	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	

Nombre	Tipo	Documentación	Propiedad
pkg: reportes	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: transporte	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: util	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: utilidades	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	

ArqCotizador. 5. Físico (despliegue)

Mi Mutual. Coomeva, 2023.

Distribución física Cotizador Web, Mi Mutual. Estado actual, 2023.

versión 0.1.1

Especificaciones de Despliegue Cotizador Web

Detalles de configuración del proyecto Mi Mutual en el espacio de trabajo local (2022).

Recursos Requeridos

- Git. Se debe instalar git para poder realizar la clonación de cada uno de los proyectos mas adelante.
- Instalación SmartGit. Se debe instalar Smartgit para poder realizar la clonación de cada uno de los proyectos mas adelante, este es opcional ya que es una interfaz gráfica de git mas amigable para el usuario en caso que no desee trabajar con la consola.
- DBeaver. Se debe instalar DBeaver para poder acceder a la base de datos.
- Instalación Maven. Se debe instalar maven para poder compilar los proyectos, nos debemos asegurar de instalar la versión 3.6.3, en caso que no se encuentra en la página oficial copiar la carpeta que esta en el repositorio a archivo de programas.
- Java 8. Se debe instalar Java para poder desplegar los proyectos mas adelante, nos debemos asegurar de instalar la versión 8.
- STS. Se debe instalar el IDE para realizar modificaciones a los proyectos back mas adelante en este caso Spring Tools 4 for Eclipse. La carpeta que genera el instalador la copiamos a archivos de programa.
- Instalación Lombok. Se debe instalar el lombok seleccionando el IDE que acabamos de instalar en este caso el STS.
- Postman. Se debe instalar el postman para poder consumir los servicios del backend mas adelante cuando ya se hayan desplegado.
- Node Js. Se debe instalar Node Js para configurar el proyecto front mas adelante, nos debemos asegurar de instalar la versión v14.2.0.
- Visual Studio Code. Se debe instalar el IDE para realizar modificaciones al proyecto front mas adelante en este caso Visual Studio code.

k. Angular 9.1.12 o superior.

Mi Mutual. Coomeva, 2023.

Distribución física Cotizador Web, Mi Mutual. Estado actual, 2023.

versión 0.1.1

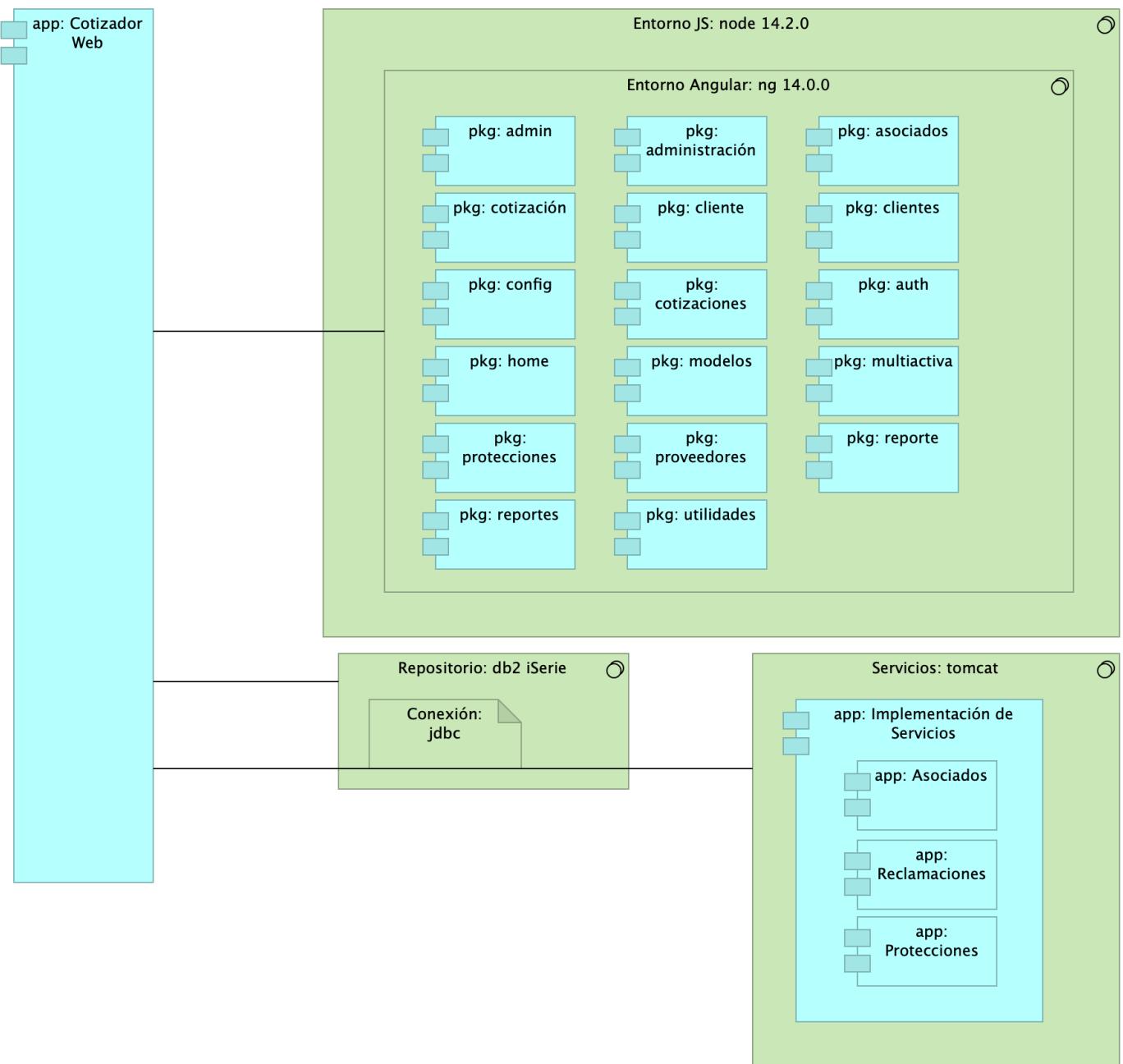


Imagen 17: ArqCotizador. 5. Físico (despliegue)

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 19: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
Conexión: jdbc	Artifact		
Entorno Angular: ng12	System Software		
Entorno JS: node 14.2.0	System Software		
Repository: db2 iSerie	System Software		
Servicios: tomcat	System Software		

Nombre	Tipo	Documentación	Propiedad
app: Asociados	Application Component	Contiene todas las funcionalidades relacionadas con consulta y creación de asociados y beneficiarios.	
app: Cotizador Web	Application Component	pkg: MiMutualWeb	
app: Implementación de Servicios	Application Component	Los componentes de este tipo se encargan de controlar y almacenar toda la lógica del negocio, validaciones y todo lo referente a procesamiento de datos.	
app: Protecciones	Application Component	Contiene todas las funcionalidades relacionadas con la gestión y configuración de productos y protecciones.	
app: Reclamaciones	Application Component	Contiene todas las funcionalidades relacionadas con la gestión de reclamaciones, liquidaciones y pagos.	
pkg: admin	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: administración	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: asociados	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: auth	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: cliente	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: clientes	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: config	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: cotizaciones	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: cotización	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: home	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: modelos	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: multiactiva	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: protecciones	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: proveedores	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	

Nombre	Tipo	Documentación	Propiedad
pkg: reporte	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: reportes	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	
pkg: utilidades	Application Component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	

ArqCotizador. 7. Datos. Negocio

Mi Mutual. Coomeva, 2023.

Mi Mutual Web. Entidades: Estructuras, objeto, relaciones con aplicación.

versión 0.1

Entidades de Negocio Mi Mutual

Dominios de datos de negocio. Entidades independiente de la plataforma y de la tecnología.

- Configuración (caracterización de productos, plan)
- Plan (producto pólizas seguros)
- Canal (medios del tomador/asociado)
- Parametros globales (catálogos)
- Portafolio de asociado
- Asociado
- Facturación
- Beneficiario

Mi Mutual. Coomeva, 2023.

Mi Mutual Web. Entidades:
Estructuras, objeto, relaciones con
aplicación.

versión 0.1

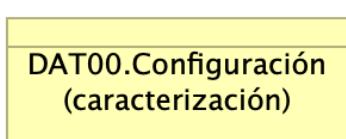
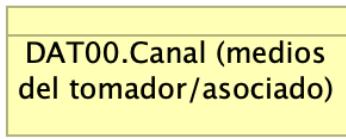
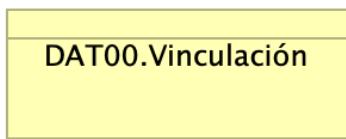
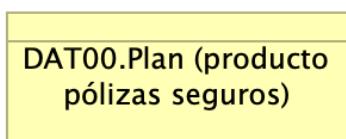
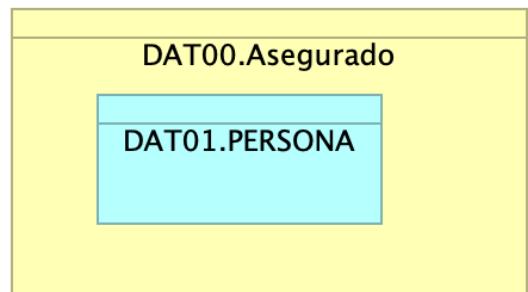
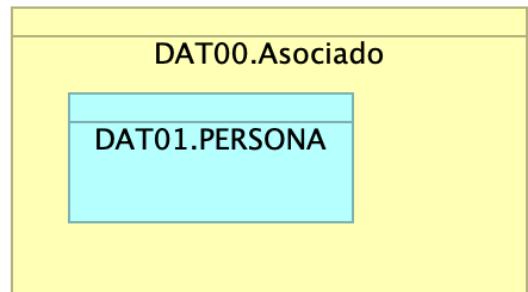
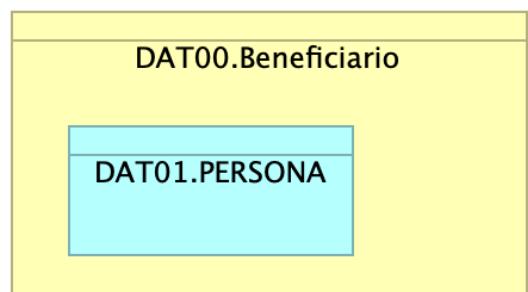
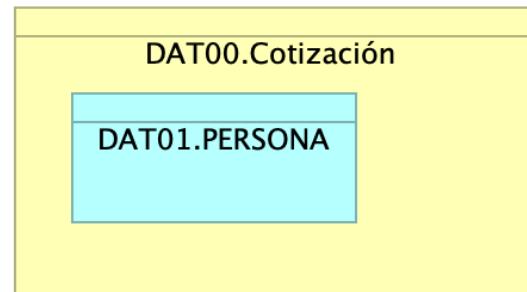


Imagen 18: ArqCotizador. 7. Datos. Negocio

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 20: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
DAT00.Asegurado	Business Object		
DAT00.Asociado	Business Object		
DAT00.Beneficiario	Business Object		
DAT00.Canal (medios del tomador/asociado)	Business Object		

Nombre	Tipo	Documentación	Propiedad
DAT00.Configuración (caracterización)	Business Object	Caracterización de productos, planes, parámetros	
DAT00.Plan (producto pólizas seguros)	Business Object		
DAT01.Cotización	Business Object		
DAT01.PERSONA	Data Object		
DAT01.Vinculación	Business Object		

Vistas de Arquitectura Mi Mutual

undefined

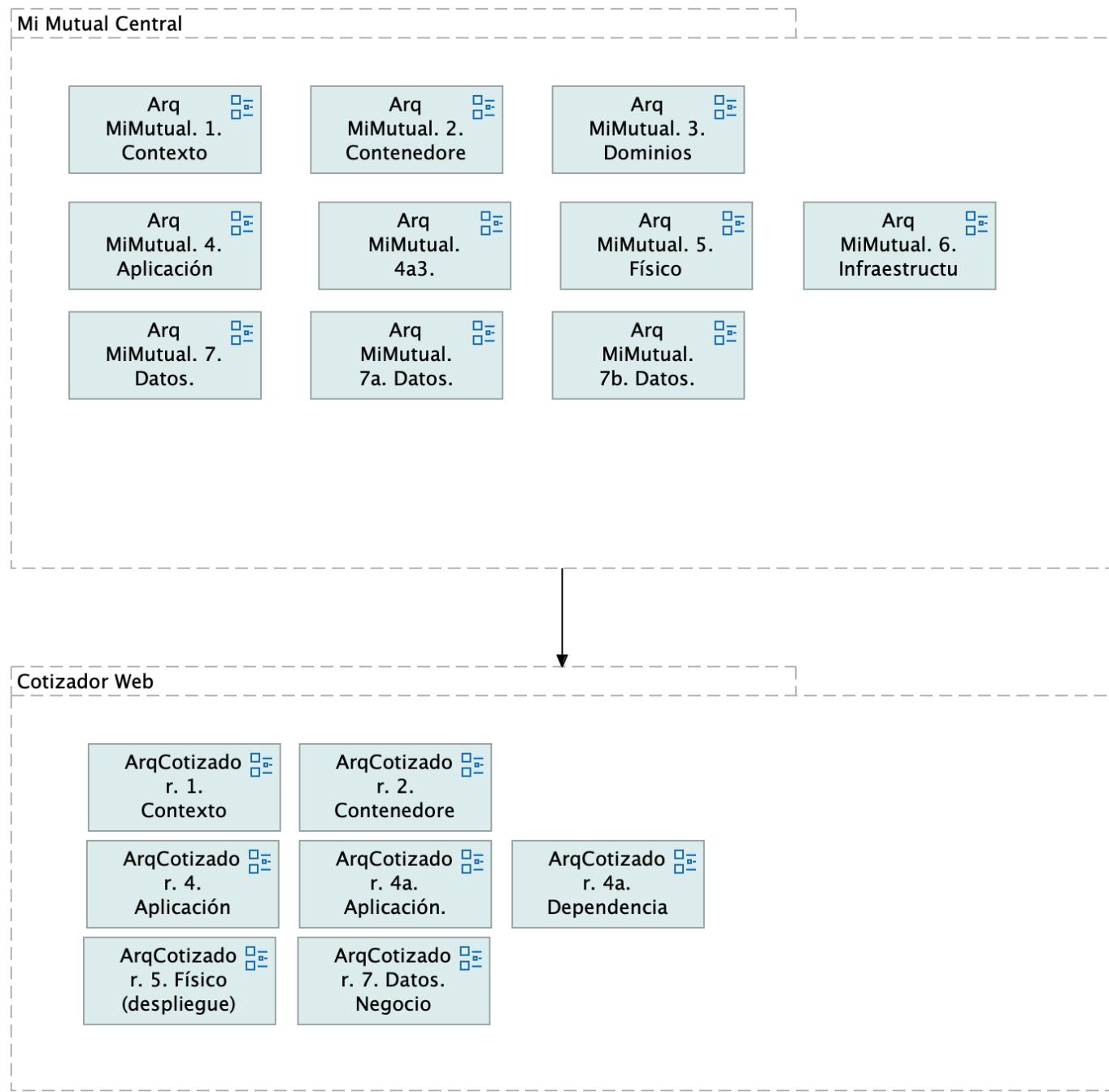


Imagen 19: Vistas de Arquitectura Mi Mutual

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 21: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
Cotizador Web	Grouping		
Mi Mutual Central	Grouping		

PGN-078

Doc.1.Datos SUI

undefined

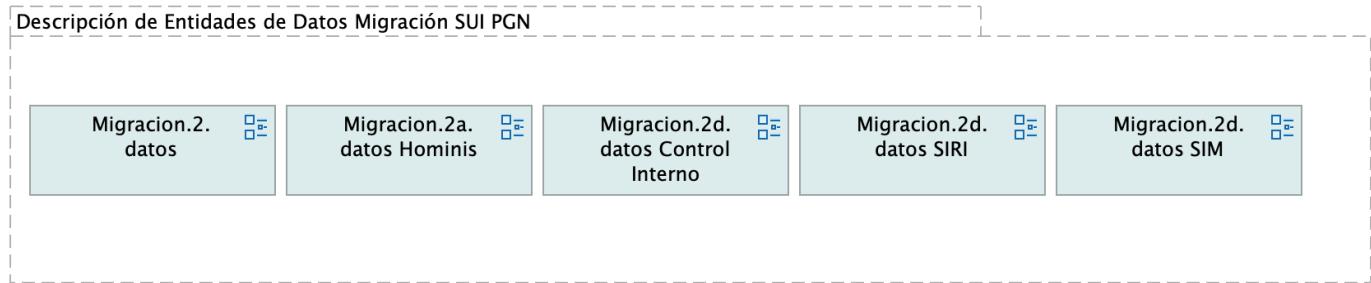


Imagen 20: Doc.1.Datos SUI

Fuente: *Repositorio arquitectura Mi Mutual (2023)*

Catálogo de Elementos

Tabla 22: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
Descripción de Entidades de Datos Migración SUI PGN	Grouping		

Doc.2.Infraestructura SUI

undefined

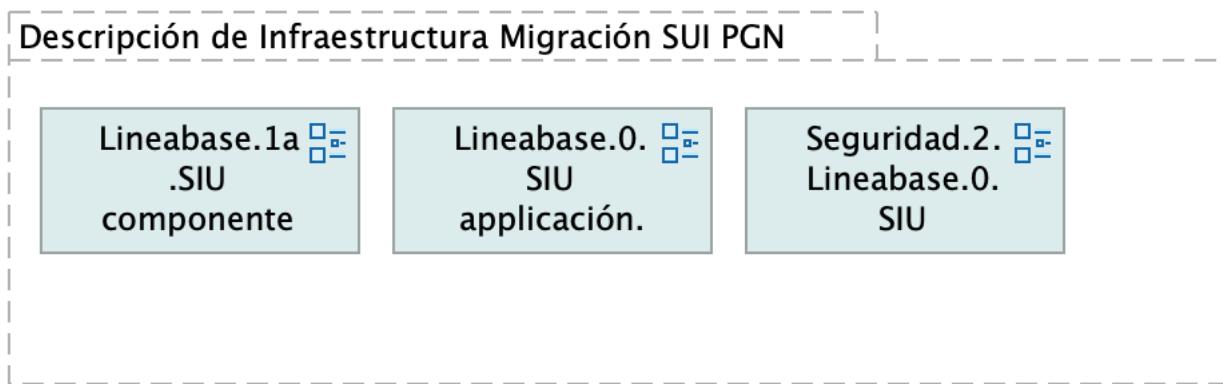


Imagen 21: Doc.2.Infraestructura SUI

Fuente: *Repositorio arquitectura Mi Mutual (2023)*

Catálogo de Elementos

Tabla 23: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
Descripción de Infraestructura Migración SUI PGN	Grouping		

Doc.3.Migración Funcional SUI

undefined

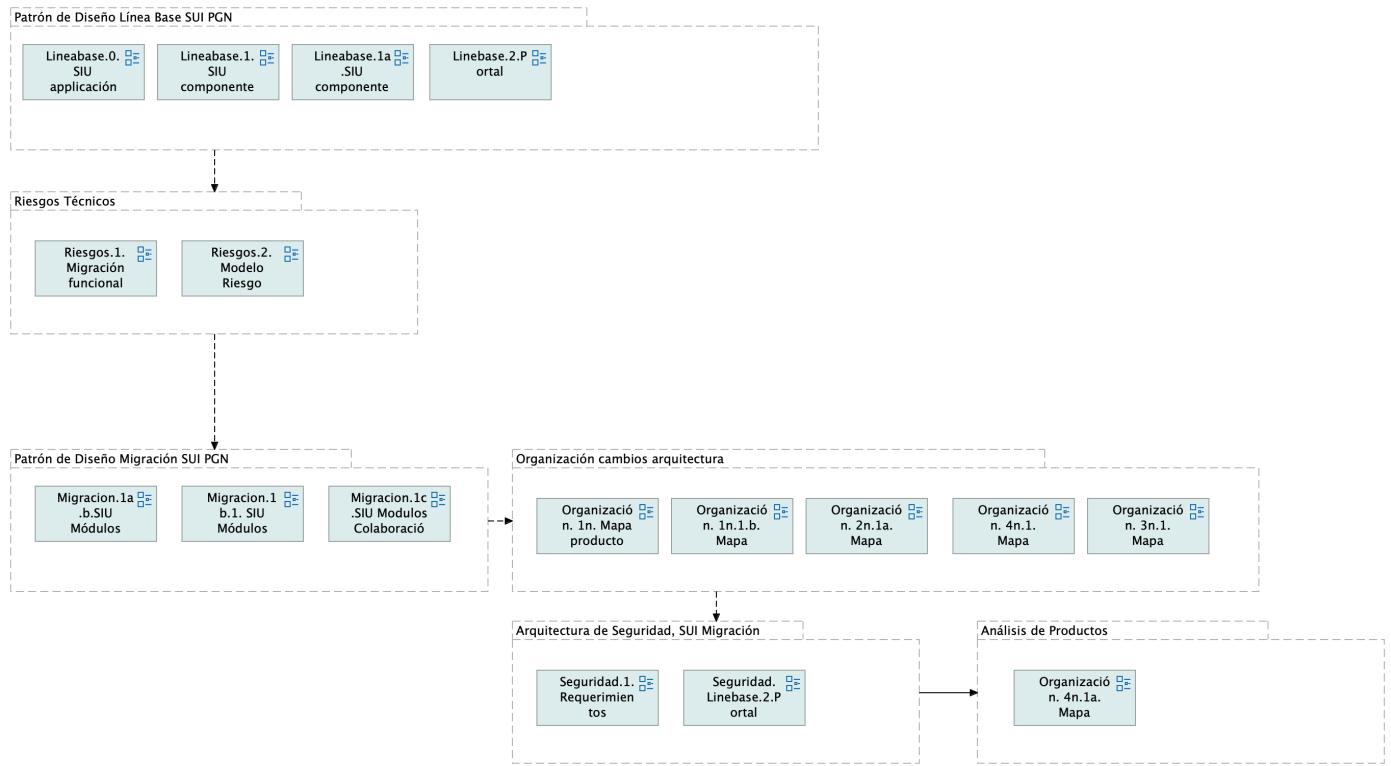


Imagen 22: Doc.3.Migración Funcional SUI

Fuente: *Repositorio arquitectura Mi Mutual (2023)*

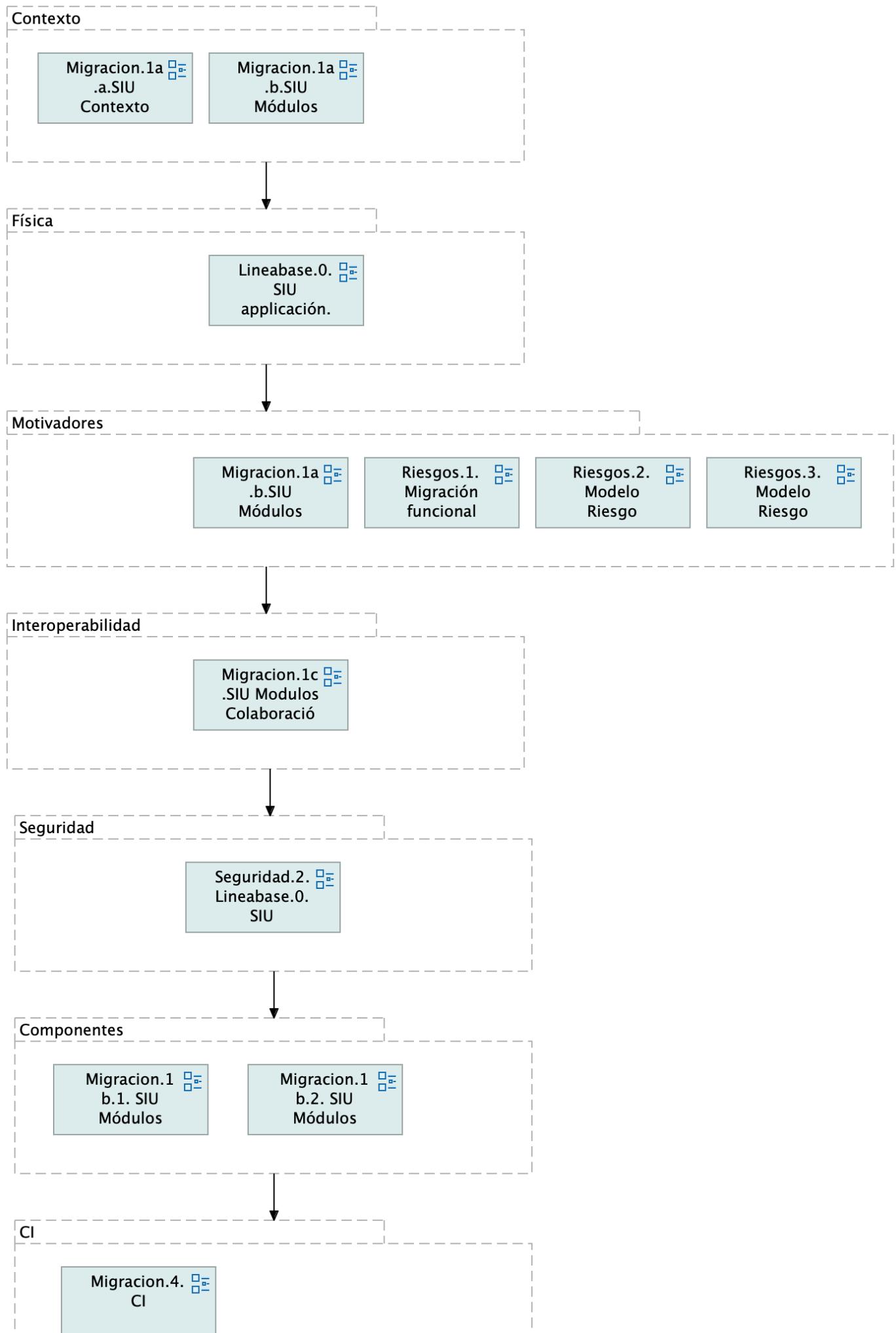
Catálogo de Elementos

Tabla 24: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
Análisis de Productos	Grouping		
Arquitectura de Seguridad, SUI Migración	Grouping		
Organización cambios arquitectura	Grouping		
Patrón de Diseño Línea Base SUI PGN	Grouping		
Patrón de Diseño Migración SUI PGN	Grouping		
Riesgos Técnicos	Grouping		

Doc.4.PGN Contractual

undefined



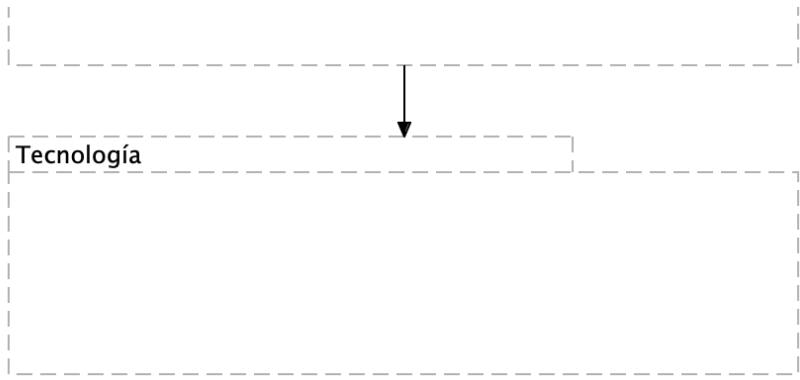


Imagen 23: Doc.4.PGN Contractual

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 25: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
CI	Grouping		
Componentes	Grouping		
Contexto	Grouping		
Física	Grouping		
Interoperabilidad	Grouping		
Motivadores	Grouping		
Seguridad	Grouping		
Tecnología	Grouping		

Lineabase.0.SIU aplicación

Procuraduría General de la Nación Proyecto Migración SIU, 2023. Fase II

Línea base sistema único de información. PGN. Componentes originales Fase I. Organización de la Aplicación.

versión 0.11

Procuraduría General de la Nación, proyecto Migración SIU, 2023, Fase II. Línea base del sistema único de información (SUI en adelante) de la PGN. Presentación de componentes de software originales implementados en la Fase I del presente proyecto.

Representación Arquitectónica

Con una arquitectura orientada a servicios SUI recopila:

1. Runtime: Es el servicio que interactúa con el usuario final (GUI) elaborado en Angular 11
2. API Tx: Servicio api rest base node encargado de realizar las transacciones básicas CRUD
3. API Config / Seguridad. Servicio Web API .Net Framework encargado de gestionar características con la autenticación y configuración

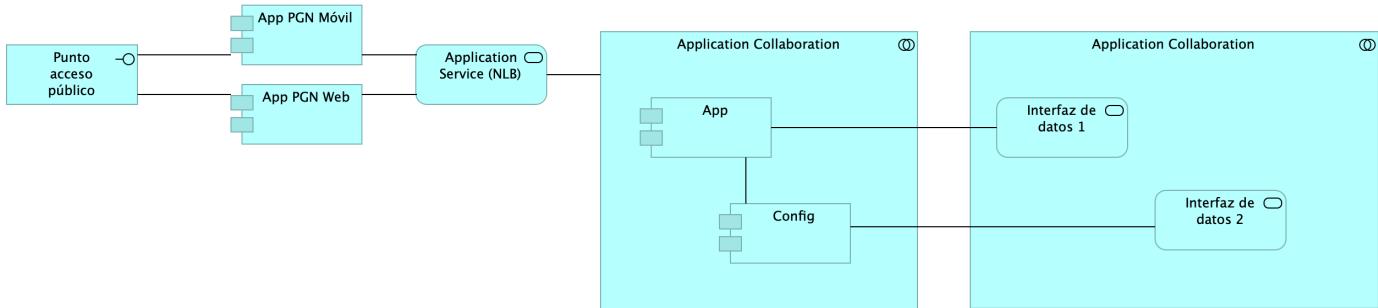
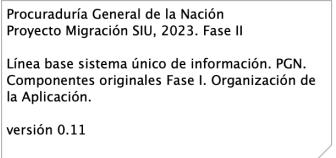


Imagen 24: Lineabase.0.SIU aplicación

Fuente: *Repositorio arquitectura Mi Mutual (2023)*

Catálogo de Elementos

Nombre	Tipo	Documentación	Propiedad
App	Application Component		
App PGN Móvil	Application Component	A partir de los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la "Guía de desarrollo OWASP" y "OWAS Cheat Sheet, se realizarán pruebas de seguridad a partir del análisis de vulnerabilidades, y pruebas de Ethikal Hacking.	

Protección de datos personales,

Los sistemas de información que recogen, procesan y almacenan información de los derechos de las personas se deben almacenar de forma adecuada, la información que pueda ser vulnerada puede generar obligaciones legales y éticas con respecto a la pérdida de información confidencial por parte de ciudadanos del país.

La información contenida en las bases de datos debe tener los mecanismos de cifrado que en otros apartados se han mencionado.
La legislación que hay que tener como referencia, ley 1581 de 2012. Decreto 1377 de 2013

La metodología empleada tendrá las siguientes fases:

- **FASE DE RECONOCIMIENTO:**

Se recolectará toda la información posible, usando diferentes técnicas como:

- o Recopilación de dominios/IPs/puertos/servicios
- o Recopilación de metadatos
- o Uso de Google Dorks.

- **ANÁLISIS DE VULNERABILIDADES:**

Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.

- **EXPLOTACIÓN:**

Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo:

- o Inyección de código
- o Inclusión de ficheros locales o remotos
- o Evasión de autenticación
- o Carencia de controles de autorización
- o Ejecución de comandos en el lado del servidor
- o Ataques tipo Cross Site Request Forgery
- o Control de errores
- o Gestión de sesiones
- o Fugas de información
- o Secuestros de sesión
- o Comprobación de las condiciones para realizar una denegación de servicio.

- **POST EXPLOTACIÓN:**

En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adicionales con el objetivo de comprobar la criticidad de esta.

No URL IP

1. https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz
135.181.185.207

| | | App PGN Web | Application Component | A partir de los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la "Guía de desarrollo OWASP" y "OWAS Cheat Sheet, se realizaran pruebas de seguridad a partir del análisis de vulnerabilidades, y pruebas de Ethical Hacking.

Los resultados permitirán identificar los requisitos de seguridad que los sistemas de información o servicios web deberán cumplir.
La metodología empleada tendrá las siguientes fases:

• FASE DE RECONOCIMIENTO:

Se recolectará toda la información posible, usando diferentes técnicas como:
o Recopilación de dominios/IPs/puertos/servicios
o Recopilación de metadatos
o Uso de Google Dorks.

• ANÁLISIS DE VULNERABILIDADES:

Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.

• EXPLOTACIÓN:

• Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo:
o Inyección de código
o Inclusión de ficheros locales o remotos
o Evasión de autenticación
o Carencia de controles de autorización
o Ejecución de comandos en el lado del servidor
o Ataques tipo Cross Site Request Forgery
o Control de errores
o Gestión de sesiones
o Fugas de información
o Secuestros de sesión
o Comprobación de las condiciones para realizar una denegación de servicio.

• POST EXPLOTACIÓN:

En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adicionales con el objetivo de comprobar la criticidad de esta.

No URL IP

1. https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz
135.181.185.207

El Login deberá evidenciar el control de errores, al momento de realizar la validación deberá mensaje de error para el caso que se autentique con credenciales erradas. | | | Application Collaboration | Application Collaboration | | | Application Collaboration | Application Collaboration | | | Application Service (NLB) | Application Service | | | Config | Application Component | | | Interfaz de datos 1 | Application Service | | | Interfaz de datos 2 | Application Service | | | Punto acceso público | Application Interface | URL tipo C
HTTP | |

Table: Elementos de la vista. {#tbl:tblelement-Lineabase.0.SIUaplicación-id}

Lineabase.0.SIU aplicación. física

Procuraduría General de la Nación Proyecto Migración SIU, 2023. Fase II

Línea base sistema único de información. PGN. Componentes originales Fase I.

versión 0.11.1

Procuraduría General de la Nación (PGN), módulo SIU migrado, 2023. Elementos físicos que soportan a la aplicación Sistema de Información Único (SIU en adelante) de la PGN, actual Fase I y existente en Fase II. Presentación de componentes de software y tecnología física (hardware) implementados en la Fase I y requeridos por Fase II (presente proyecto).

Representación Arquitectónica

Con una arquitectura orientada a servicios SUI recopila:

1. Runtime: Es el servicio que interactúa con el usuario final (GUI) elaborado en Angular 11
2. API Tx: Servicio API rest base node encargado de realizar las transacciones básicas CRUD
3. API Config / Seguridad. Servicio Web API .Net Framework encargado de gestionar características con la autenticación y configuración

Procuraduría General de la Nación
 Proyecto Migración SIU, 2023. Fase II
 Línea base sistema único de información. PGN.
 Componentes originales Fase I.
 versión 0.11.1

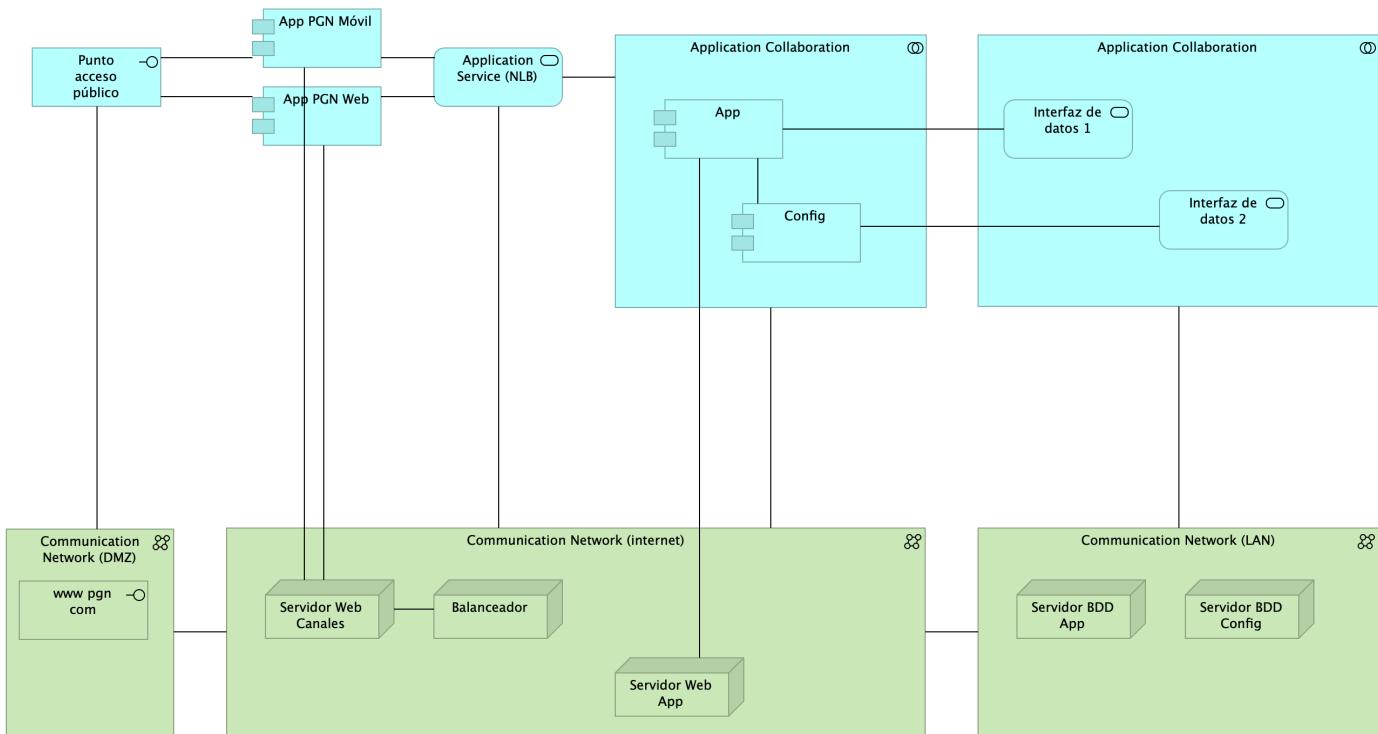


Imagen 25: Lineabase.0.SIU aplicación. física

Fuente: *Repositorio arquitectura Mi Mutual (2023)*

Catálogo de Elementos

Nombre	Tipo	Documentación	Propiedad
App	Application Component		
App PGN Móvil	Application Component	A partir de los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la "Guía de desarrollo OWASP" y "OWAS Cheat Sheet, se realizarán pruebas de seguridad a partir del análisis de vulnerabilidades, y pruebas de Ethikal Hacking.	

Protección de datos personales,

Los sistemas de información que recogen, procesan y almacenan información de los derechos de las personas se deben almacenar de forma adecuada, la información que pueda ser vulnerada puede generar obligaciones legales y éticas con respecto a la pérdida de información confidencial por parte de ciudadanos del país.

La información contenida en las bases de datos debe tener los mecanismos de cifrado que en otros apartados se han mencionado. La legislación que hay que tener como referencia, ley 1581 de 2012. Decreto 1377 de 2013

La metodología empleada tendrá las siguientes fases:

• FASE DE RECONOCIMIENTO:

Se recolectará toda la información posible, usando diferentes técnicas como:

- o Recopilación de dominios/ IPs/puertos/servicios
- o Recopilación de metadatos
- o Uso de Google Dorks.

• ANÁLISIS DE VULNERABILIDADES:

Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.

• EXPLOTACIÓN:

- Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo:
 - Inyección de código
 - Inclusión de ficheros locales o remotos
 - Evasión de autenticación
 - Carencia de controles de autorización
 - Ejecución de comandos en el lado del servidor
 - Ataques tipo Cross Site Request Forgery
 - Control de errores
 - Gestión de sesiones
 - Fugas de información
 - Secuestros de sesión
 - Comprobación de las condiciones para realizar una denegación de servicio.

• POST EXPLOTACIÓN:

En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adicionales con el objetivo de comprobar la criticidad de esta.

No URL IP

1. https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz

135.181.185.207

| | | App PGN Web | Application Component | A partir de los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la "Guía de desarrollo OWASP" y "OWAS Cheat Sheet, se realizaran pruebas de seguridad a partir del análisis de vulnerabilidades, y pruebas de Ethical Hacking.

Los resultados permitirán identificar los requisitos de seguridad que los sistemas de información o servicios web deberán cumplir.

La metodología empleada tendrá las siguientes fases:

• FASE DE RECONOCIMIENTO:

Se recolectará toda la información posible, usando diferentes técnicas como:

- Recopilación de dominios/ IPs/puertos/servicios
- Recopilación de metadatos
- Uso de Google Dorks.

• ANÁLISIS DE VULNERABILIDADES:

Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.

• EXPLOTACIÓN:

• Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo:

- Inyección de código
- Inclusión de ficheros locales o remotos
- Evasión de autenticación
- Carencia de controles de autorización
- Ejecución de comandos en el lado del servidor
- Ataques tipo Cross Site Request Forgery
- Control de errores
- Gestión de sesiones
- Fugas de información
- Secuestros de sesión
- Comprobación de las condiciones para realizar una denegación de servicio.

• POST EXPLOTACIÓN:

En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adicionales con el objetivo de comprobar la criticidad de esta.

No URL IP

1. https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz

135.181.185.207

El Login deberá evidenciar el control de errores, al momento de realizar la validación deberá mensaje de error para el caso que se autentique con credenciales erradas. | | | Application Collaboration | Application Collaboration | | | Application Collaboration | Application Collaboration | | | Application Service (NLB) | Application Service | | | Balanceador | Node | | | Communication Network (DMZ) | Communication Network | | | Communication Network (LAN) | Communication Network | | | Communication Network (internet) | Communication Network | | | Config | Application Component | | | Interfaz de datos 1 | Application Service | | | Interfaz de datos 2 | Application Service | | | Punto acceso público | Application Interface | URL tipo C

HTTP | | | Servidor BDD App | Node | Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz Discos SO C: 126 GB, Backup E: 511 GB, SQL Data F: 510 GB, SQL Log G: 510 GB, TempDB H: 63.6 GB.

| | | Servidor BDD Config | Node | Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz Discos SO C: 80 GB, Backup E: 250 GB, SQL Data F: 250 GB, SQL Log G: 250 GB, TempDB H: 30 GB.

| | | Servidor Web App | Node | Windows Server 2019 Standard o Datacenter x64. Nombre físico. IP LAN. IP Pública. Windows Server 2019 Standard or Datacenter x64. RAM 8 GB. CPU 64 Bits. 4 Cores de 2 Ghz. Discos SO C: 126 GB. SO D: 16 GB.

| | | Servidor Web Canales | Node | Windows Server 2019 Standard o Datacenter x64. Nombre físico. IP LAN. IP Pública. Windows Server 2019 Standard or Datacenter x64. RAM 8 GB. CPU 64 Bits. 4 Cores de 2 Ghz. Discos SO C: 126 GB. SO D: 16 GB.

| | | www.pgn.com | Technology Interface | | |

Table: Elementos de la vista. {#tbl:tblelement-Lineabase.0.SIUaplicación.física-id}

Lineabase.1.SIU componente

Distribución de los servicios y paquetes que integran la aplicación de SUI.

Cuatro paquetes con tecnologías respectivas

1. Angular 11 (Web)
2. API Transaccional (Node Js)
3. API Config (C#)
4. Persistencia (SQL)

Asuntos de la Migración:

- Estrategia CMS central
- Motor de búsqueda
- Estatego como BI
- Conciliación y Doku
- Gestión de sesiones / caducidad

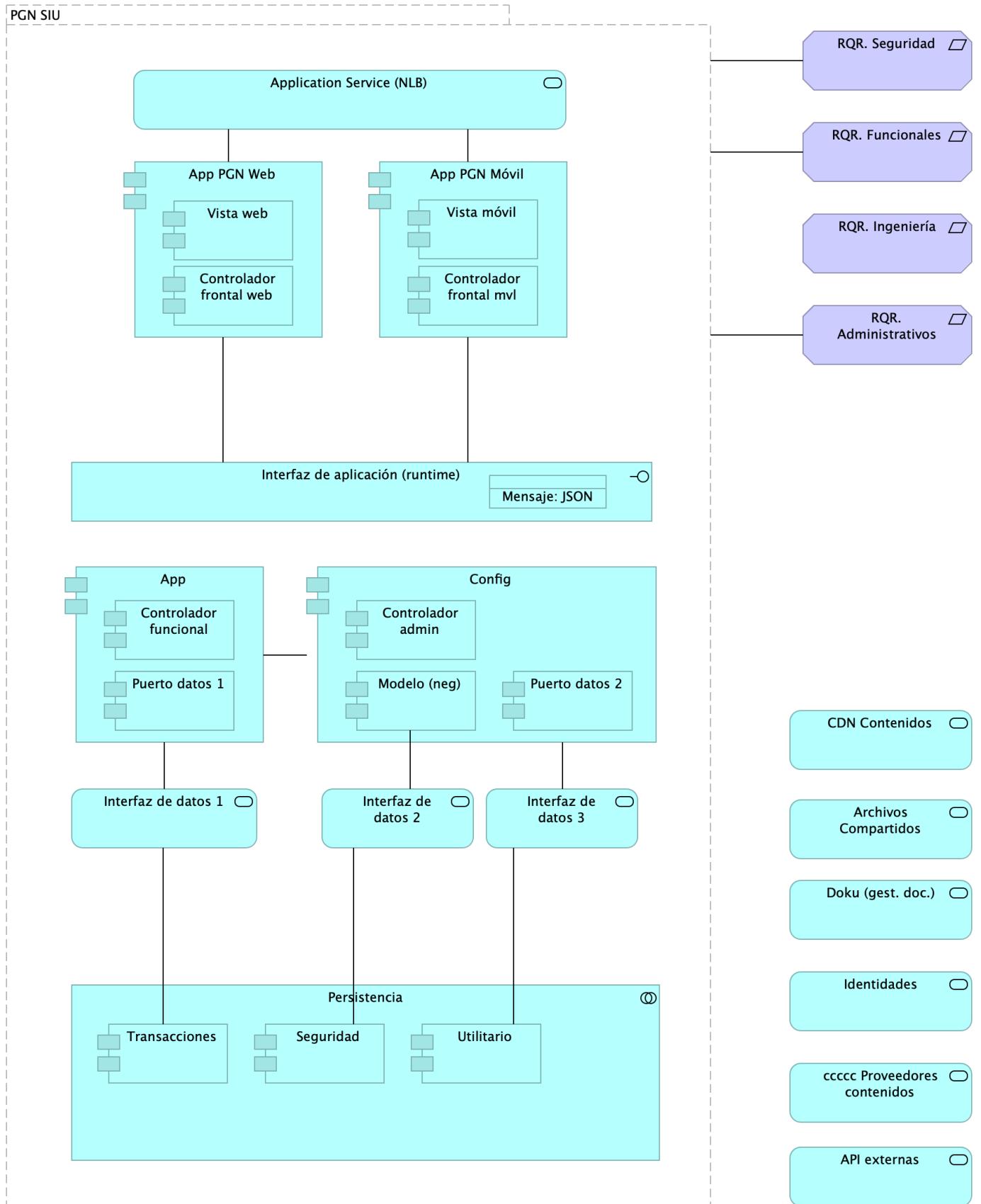


Imagen 26: Lineabase.1.SIU componente

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Nombre	Tipo	Documentación	Propiedad
API externas	Application Service		

Nombre	Tipo	Documentación	Propiedad
App	Application Component		
App PGN Móvil	Application Component	A partir de los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la "Guía de desarrollo OWASP" y "OWAS Cheat Sheet, se realizaran pruebas de seguridad a partir del análisis de vulnerabilidades, y pruebas de Ethical Hacking.	

Protección de datos personales,

Los sistemas de información que recogen, procesan y almacenan información de los derechos de las personas se deben almacenar de forma adecuada, la información que pueda ser vulnerada puede generar obligaciones legales y éticas con respecto a la pérdida de información confidencial por parte de ciudadanos del país.

La información contenida en las bases de datos debe tener los mecanismos de cifrado que en otros apartados se han mencionado.

La legislación que hay que tener como referencia, ley 1581 de 2012. Decreto 1377 de 2013

La metodología empleada tendrá las siguientes fases:

- FASE DE RECONOCIMIENTO:

Se recolectará toda la información posible, usando diferentes técnicas como:

- o Recopilación de dominios/IPs/puertos/servicios
- o Recopilación de metadatos
- o Uso de Google Dorks.

- ANÁLISIS DE VULNERABILIDADES:

Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.

- EXPLOTACIÓN:

Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo:

- o Inyección de código
- o Inclusión de ficheros locales o remotos
- o Evasión de autenticación
- o Carencia de controles de autorización
- o Ejecución de comandos en el lado del servidor
- o Ataques tipo Cross Site Request Forgery
- o Control de errores
- o Gestión de sesiones
- o Fugas de información
- o Secuestros de sesión
- o Comprobación de las condiciones para realizar una denegación de servicio.

- POST EXPLOTACIÓN:

En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adicionales con el objetivo de comprobar la criticidad de esta.

No URL IP

1. https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz

135.181.185.207

| | | App PGN Web | Application Component | A partir de los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la "Guía de desarrollo OWASP" y "OWAS Cheat Sheet, se realizaran pruebas de seguridad a partir del análisis de vulnerabilidades, y pruebas de Ethical Hacking.

Los resultados permitirán identificar los requisitos de seguridad que los sistemas de información o servicios web deberán cumplir.

La metodología empleada tendrá las siguientes fases:

- FASE DE RECONOCIMIENTO:

Se recolectará toda la información posible, usando diferentes técnicas como:

- o Recopilación de dominios/IPs/puertos/servicios
- o Recopilación de metadatos
- o Uso de Google Dorks.

- ANÁLISIS DE VULNERABILIDADES:

Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.

- EXPLOTACIÓN:

Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo:

- o Inyección de código
- o Inclusión de ficheros locales o remotos
- o Evasión de autenticación
- o Carencia de controles de autorización
- o Ejecución de comandos en el lado del servidor

- o Ataques tipo Cross Site Request Forgery
- o Control de errores
- o Gestión de sesiones
- o Fugas de información
- o Secuestros de sesión
- o Comprobación de las condiciones para realizar una denegación de servicio.

• POST EXPLOTACIÓN:

En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adicionales con el objetivo de comprobar la criticidad de esta.

No URL IP

1. https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz
135.181.185.207

El Login deberá evidenciar el control de errores, al momento de realizar la validación deberá mensaje de error para el caso que se autentique con credenciales erradas. | | | Application Service (NLB) | Application Service | | | Archivos Compartidos | Application Service | | | CDN Contenidos | Application Service | | | Config | Application Component | | | Controlador admin | Application Component | | | Controlador frontal mvl | Application Component | | | Controlador frontal web | Application Component | - Verificados los SSL, se recomienda adquirir SSL seguros, con entidades certificadoras.

Si se desea continuar con SSL de Let's Encrypt, se recomienda automatizar el proceso de actualización dado que al dejar estos en modo actualización manual es probable el olvido de esta actualización (Estos certificados se deben actualizar trimestralmente y no cuentan con las características de seguridad necesarias).

| | | Controlador funcional | Application Component | | | Doku (gest. doc.) | Application Service | | | Identidades | Application Service | | | Interfaz de aplicación (runtime) | Application Interface | Servidor web: Microsoft-IIS/10.0

Marco de Programación: ASP.NET

Huellas digitales identificadas:

Huella digital SHA-256 "FC:79:06:7E:F5:24:20:50:F1:C0:74:F7:85:56:B9:05:B7:33:A3:2D:44:A0:48"

Huella digital SHA1 "8C:48:BD:E2:F5:18:18:C3:85:96:68:44:2E:28:A0:68:08:2F:0A:BE"

| | | Interfaz de datos 1 | Application Service | | | Interfaz de datos 2 | Application Service | | | Interfaz de datos 3 | Application Service | | | Mensaje: JSON | Data Object | | | Modelo (neg) | Application Component | | | PGN SIU | Grouping | El objetivo principal de la arquitectura del SUI de la migración es la centralización de los conceptos misionales: concentrar los conceptos misionales en componentes aislados; dejar por fuera de estos componentes misionales todo lo distintos a la misionalidad de la PGN.

Los objetivos secundarios de esta arquitectura SUI de la migración son flexibilidad y extensibilidad. Dichos objetivos son independientes. Es decir, estos pueden ser maximizados sin conflicto entre ellos.

| | | Persistencia | Application Collaboration | | | Puerto datos 1 | Application Component | | | Puerto datos 2 | Application Component | | | RQR. Administrativos | Requirement | | | RQR. Funcionales | Requirement | | | RQR. Ingeniería | Requirement | | | RQR. Seguridad | Requirement | Requerimientos de seguridad, SUI, Migración, en aspectos de comunicación, autenticación, autorización y (manejo de) sesiones.

| | | Seguridad | Application Component | | | Transacciones | Application Component | | | Utilitario | Application Component | | | Vista móvil | Application Component | | | Vista web | Application Component | - Verificados los SSL, se recomienda adquirir SSL seguros, con entidades certificadoras.

Si se desea continuar con SSL de Let's Encrypt, se recomienda automatizar el proceso de actualización dado que al dejar estos en modo actualización manual es probable el olvido de esta actualización (Estos certificados se deben actualizar trimestralmente y no cuentan con las características de seguridad necesarias).

4. SERVICIOS IDENTIFICADOS:

Servidor web: Microsoft-IIS/10.0

Marco de Programación: ASP.NET

Huellas digitales identificadas:

Huella digital SHA-256 "FC:79:06:7E:F5:24:20:50:F1:C0:74:F7:85:56:B9:05:B7:33:A3:2D:44:A0:48"

Huella digital SHA1 "8C:48:BD:E2:F5:18:18:C3:85:96:68:44:2E:28:A0:68:08:2F:0A:BE"

| | | ccccc Proveedores contenidos | Application Service | | |

Table: Elementos de la vista. {#tbl:tblelement-Lineabase.1.SIUcomponente-id}

Lineabase.1a.SIU componentes. infraestructura

Dependencias de infraestructura entre los servicios que integran el modelo de aplicación de SUI, Migración.

- Servidor de Canales (App PGN web y móvil)
- Servidor Web App (App SUI)
- Servidor Lappiz (Config SUI)
- Servidor BDD App (Transaccional)
- Servidor BDD Config (Configuración)

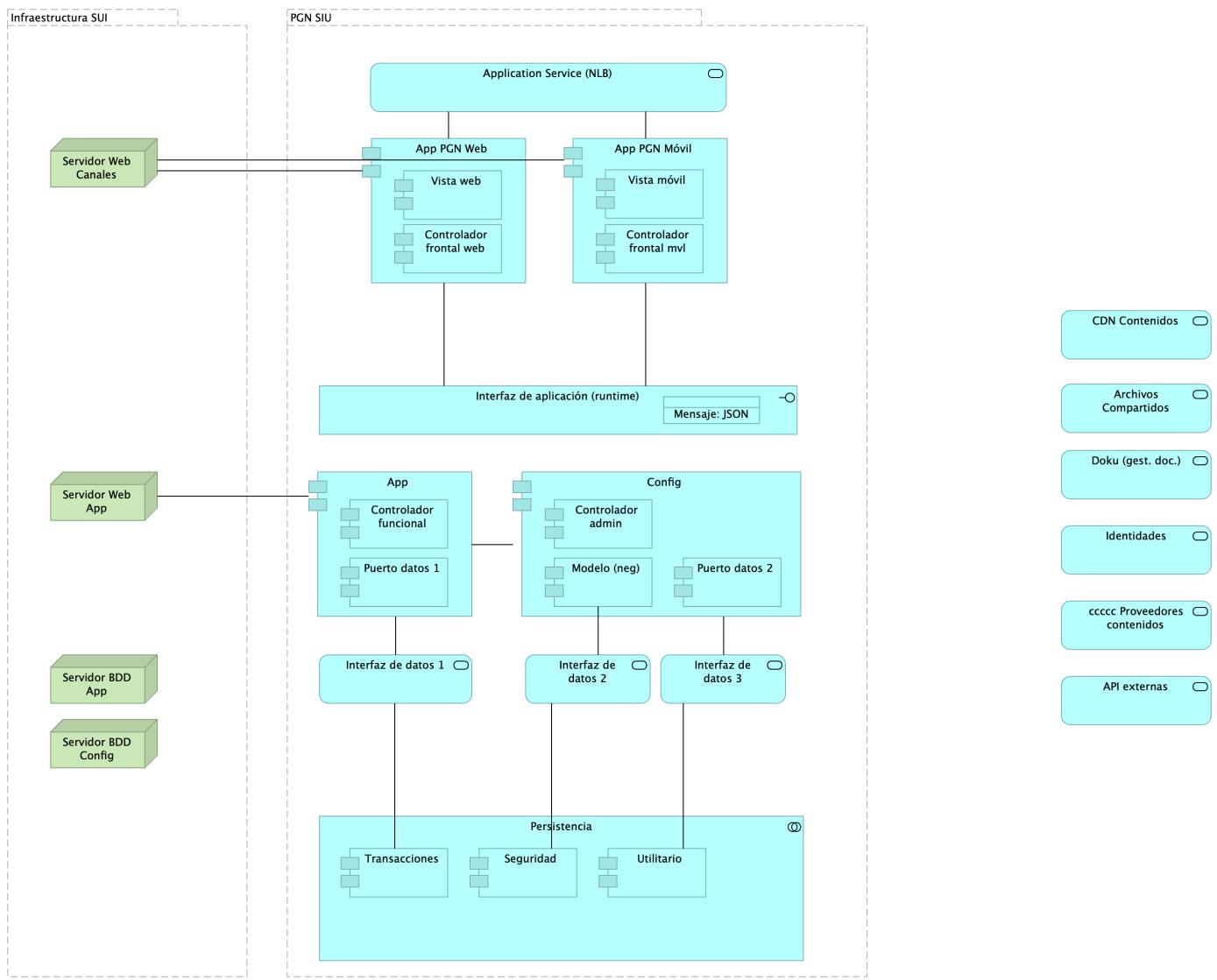


Imagen 27: Lineabase.1a.SIU componentes. infraestrutura

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Nombre	Tipo	Documentación	Propiedad
API externas	Application Service		
App	Application Component		
App PGN Móvil	Application Component	A partir de los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la "Guía de desarrollo OWASP" y "OWAS Cheat Sheet, se realizarán pruebas de seguridad a partir del análisis de vulnerabilidades, y pruebas de Ethical Hacking.	

Protección de datos personales,

Los sistemas de información que recogen, procesan y almacenan información de los derechos de las personas se deben almacenar de forma adecuada, la información que pueda ser vulnerada puede generar obligaciones legales y éticas con respecto a la pérdida de información confidencial por parte de ciudadanos del país.

La información contenida en las bases de datos debe tener los mecanismos de cifrado que en otros apartados se han mencionado.
La legislación que hay que tener como referencia, ley 1581 de 2012. Decreto 1377 de 2013

La metodología empleada tendrá las siguientes fases:

- FASE DE RECONOCIMIENTO:

Se recolectará toda la información posible, usando diferentes técnicas como:

- o Recopilación de dominios/IPs/puertos/servicios
- o Recopilación de metadatos
- o Uso de Google Dorks.

• ANÁLISIS DE VULNERABILIDADES:

Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.

• EXPLOTACIÓN:

- Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo:
 - o Inyección de código
 - o Inclusión de ficheros locales o remotos
 - o Evasión de autenticación
 - o Carencia de controles de autorización
 - o Ejecución de comandos en el lado del servidor
 - o Ataques tipo Cross Site Request Forgery
 - o Control de errores
 - o Gestión de sesiones
 - o Fugas de información
 - o Secuestros de sesión
 - o Comprobación de las condiciones para realizar una denegación de servicio.

• POST EXPLOTACIÓN:

En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adicionales con el objetivo de comprobar la criticidad de esta.

No URL IP

1. https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz
135.181.185.207

| | | App PGN Web | Application Component | A partir de los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la "Guía de desarrollo OWASP" y "OWAS Cheat Sheet", se realizarán pruebas de seguridad a partir del análisis de vulnerabilidades, y pruebas de Ethical Hacking.

Los resultados permitirán identificar los requisitos de seguridad que los sistemas de información o servicios web deberán cumplir.

La metodología empleada tendrá las siguientes fases:

• FASE DE RECONOCIMIENTO:

- Se recolectará toda la información posible, usando diferentes técnicas como:
- o Recopilación de dominios/IPs/puertos/servicios
 - o Recopilación de metadatos
 - o Uso de Google Dorks.

• ANÁLISIS DE VULNERABILIDADES:

Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.

• EXPLOTACIÓN:

- Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo:
 - o Inyección de código
 - o Inclusión de ficheros locales o remotos
 - o Evasión de autenticación
 - o Carencia de controles de autorización
 - o Ejecución de comandos en el lado del servidor
 - o Ataques tipo Cross Site Request Forgery
 - o Control de errores
 - o Gestión de sesiones
 - o Fugas de información
 - o Secuestros de sesión
 - o Comprobación de las condiciones para realizar una denegación de servicio.

• POST EXPLOTACIÓN:

En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adicionales con el objetivo de comprobar la criticidad de esta.

No URL IP

1. https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz
135.181.185.207

El Login deberá evidenciar el control de errores, al momento de realizar la validación deberá mensaje de error para el caso que se autentique con credenciales erradas. | | | Application Service (NLB) | Application Service | | | Archivos Compartidos | Application Service | | | CDN Contenidos | Application Service | | | Config | Application Component | | | Controlador admin | Application Component | | | Controlador frontal mvl | Application Component | | | Controlador frontal web | Application Component | - Verificados los SSL, se recomienda adquirir SSL seguros, con entidades certificadoras.

Si se desea continuar con SSL de Let's Encrypt, se recomienda automatizar el proceso de actualización dado que al dejar estos en modo actualización manual es probable el olvido de esta actualización (Estos certificados se deben actualizar trimestralmente y no cuentan con las características de seguridad necesarias).

| | | Controlador funcional | Application Component | | | Doku (gest. doc.) | Application Service | | | Identidades | Application Service | | |

Infraestructura SUI | Grouping | Soporte de infraestructura a los componentes del SUI Migración. Servidores y ambientes de cómputo para la ejecución del software base de los componentes misionales del SUI de PGN.

| | | Interfaz de aplicación (runtime) | Application Interface | Servidor web: Microsoft-IIS/10.0

Marco de Programación: ASP.NET

Huellas digitales identificadas:

Huella digital SHA-256 "FC:79:06:7E:F5:24:20:50:F1:C0:74:F7:85:56:B9:05:B7:33:A3:2D:44:A0:48"

Huella digital SHA1 "8C:48:BD:E2:F5:18:18:C3:85:96:68:44:2E:28:A0:68:08:2F:0A:BE"

| | | Interfaz de datos 1 | Application Service | | | | Interfaz de datos 2 | Application Service | | | | Interfaz de datos 3 | Application Service | | | | Mensaje: JSON | Data Object | | | | Modelo (neg) | Application Component | | | | PGN SIU | Grouping | El objetivo principal de la arquitectura del SUI de la migración es la centralización de los conceptos misionales: concentrar los conceptos misionales en componentes aislados; dejar por fuera de estos componentes misionales todo lo distintos a la misionalidad de la PGN.

Los objetivos secundarios de esta arquitectura SUI de la migración son flexibilidad y extensibilidad. Dichos objetivos son independientes. Es decir, estos pueden ser maximizados sin conflicto entre ellos.

| | | Persistencia | Application Collaboration | | | | Puerto datos 1 | Application Component | | | | Puerto datos 2 | Application Component | | | | Seguridad | Application Component | | | | Servidor BDD App | Node | Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz

Discos SO C: 126 GB, Backup E: 511 GB, SQL Data F: 510 GB, SQL Log G: 510 GB, TempDB G: 63.6 GB.

| | | | Servidor BDD Config | Node | Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz

Discos SO C: 80 GB, Backup E: 250 GB, SQL Data F: 250 GB, SQL Log G: 250 GB, TempDB G: 30 GB.

| | | | Servidor Web App | Node | Windows Server 2019 Standard o Datacenter x64. Nombre físico. IP LAN. IP Pública. Windows Server 2019 Standard or Datacenter x64. RAM 8 GB. CPU 64 Bits. 4 Cores de 2 Ghz. Discos SO C: 126 GB. SO D: 16 GB.

| | | | Servidor Web Canales | Node | Windows Server 2019 Standard o Datacenter x64. Nombre físico. IP LAN. IP Pública. Windows Server 2019 Standard or Datacenter x64. RAM 8 GB. CPU 64 Bits. 4 Cores de 2 Ghz. Discos SO C: 126 GB. SO D: 16 GB.

| | | | Transacciones | Application Component | | | | Utilitario | Application Component | | | | Vista móvil | Application Component | | | | Vista web | Application Component | - Verificados los SSL, se recomienda adquirir SSL seguros, con entidades certificadoras.

Si se desea continuar con SSL de Let's Encrypt, se recomienda automatizar el proceso de actualización dado que al dejar estos en modo actualización manual es probable el olvido de esta actualización (Estos certificados se deben actualizar trimestralmente y no cuentan con las características de seguridad necesarias.

4. SERVICIOS IDENTIFICADOS:

Servidor web: Microsoft-IIS/10.0

Marco de Programación: ASP.NET

Huellas digitales identificadas:

Huella digital SHA-256 "FC:79:06:7E:F5:24:20:50:F1:C0:74:F7:85:56:B9:05:B7:33:A3:2D:44:A0:48"

Huella digital SHA1 "8C:48:BD:E2:F5:18:18:C3:85:96:68:44:2E:28:A0:68:08:2F:0A:BE"

| | | cccc Proveedores contenidos | Application Service | | |

Table: Elementos de la vista. {#tbl:tblelement-Lineabase.1a.SIUcomponentes.infraestrutura-id}

Linebase.2.Portal

El portal es el conjunto de los elementos físicos y lógicos necesarios para la implementación de la granja de servidores de SharePoint Server 2019 para el portal de la PROCURADURIA.

- Servidores Web Front End
- Servidores de Aplicaciones
- Servidores de SQL Server

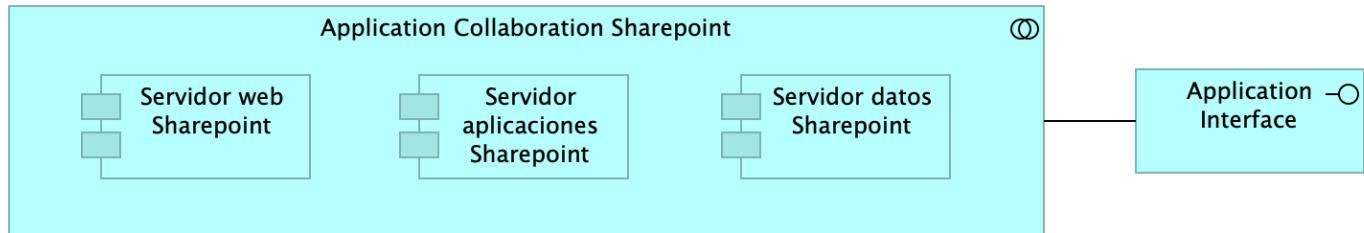


Imagen 28: Linebase.2.Portal

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 26: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
Application Collaboration Sharepoint	Application Collaboration		
Application Interface	Application Interface		

Nombre	Tipo	Documentación	Propiedad
Servidor aplicaciones Sharepoint	Application Component		
Servidor datos Sharepoint	Application Component		
Servidor web Sharepoint	Application Component		

Migracion.1a.a.SIU Contexto

PGN. Migración Sistemas Misionales. Fase 2.

Submódulos Sistema Único de Información. Requerimientos asociados a submódulos.

versión 0.4

La vista presenta en contexto a los módulos SUI migrados y el estilo de comunicación vía API sincronica/asincrónica.

Cada módulo migrado atiende al funcionario que le corresponde, p. ejemplo, Relatoría atiende a la dependencia Jurídica de la PGN. Los módulos comparten su información mediante el API local presente dentro de cada uno. Esto es, la información se mantiene protegida en dominios pero coordinada (se comparte con otros dominios).

El arreglo de datos de registros operativos y transaccionales es como sigue: cada módulo individual mantiene su registro de datos, estado y transacciones minimizado y protegido (individual y aislado). Salvo excepciones no consentidas por el diseño original, un módulo puede compartir el mismo almacen de datos con otro.

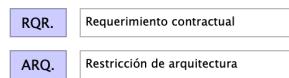
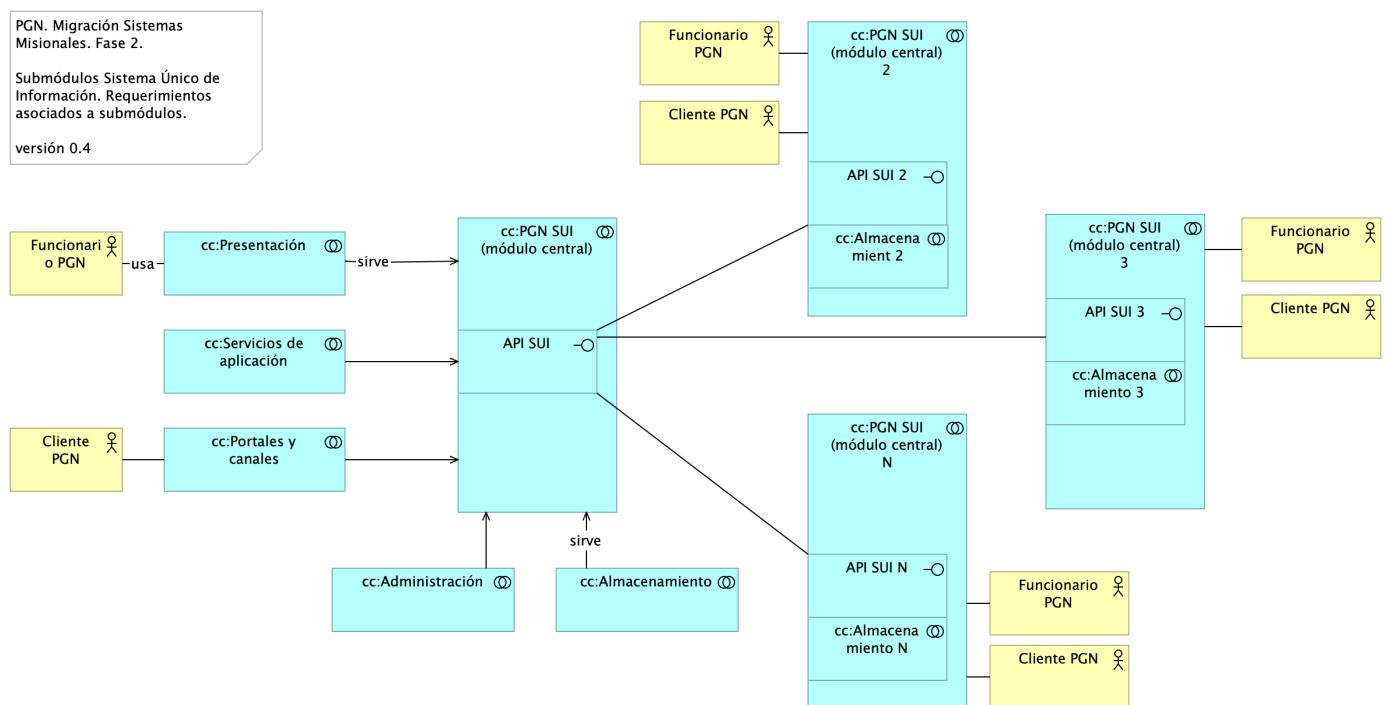


Imagen 29: Migracion.1a.a.SIU Contexto

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 27: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
--------	------	---------------	-----------

Nombre	Tipo	Documentación	Propiedad
API SUI	Application Interface	API de representación del módulo. Centralización de la comunicación con otros módulos del SUI migrado.	
API SUI 2	Application Interface	API de representación del módulo. Centralización de la comunicación con otros módulos del SUI migrado.	
API SUI 3	Application Interface	API de representación del módulo. Centralización de la comunicación con otros módulos del SUI migrado.	
API SUI N	Application Interface	API de representación del módulo. Centralización de la comunicación con otros módulos del SUI migrado.	
Cliente PGN	Business Actor		
Funcionario PGN	Business Actor		
cc:Administración	Application Collaboration		
cc:Almacenamiento 2	Application Collaboration	Espacio de almacenamiento operativo y transaccional de un módulo central del SUI migrado.	
cc:Almacenamiento	Application Collaboration	Espacio de almacenamiento operativo y transaccional de un módulo central del SUI migrado.	
cc:Almacenamiento 3	Application Collaboration	Espacio de almacenamiento operativo y transaccional de un módulo central del SUI migrado.	
cc:Almacenamiento N	Application Collaboration	Espacio de almacenamiento operativo y transaccional de un módulo central del SUI migrado.	
cc:PGN SUI (módulo central)	Application Collaboration	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN.	
cc:PGN SUI (módulo central) 2	Application Collaboration	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN.	
cc:PGN SUI (módulo central) 3	Application Collaboration	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN.	
cc:PGN SUI (módulo central) N	Application Collaboration	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN.	
cc:Portales y canales	Application Collaboration	Submódulo de portales internos de la PGN a donde llega el SUI. Interfaz web que usa al SUI para llegar a direcciones y subdirecciones de la PGN. La plataforma principal de portales en este contexto es Sharepoint de Microsoft.	
cc:Presentación	Application Collaboration	Submódulo de presentación del SUI. interfaz gráfica, interfaz web visible a los usuarios clientes y funcionarios de la PGN.	
cc:Servicios de aplicación	Application Collaboration	Submódulo de servicios utilitarios que sirven al SUI. Servicios variados que cumplen roles facilitadores de las actividades misionales del SUI. Ejemplos de estos servicios son los de gestión documental, implementado por Doku en el contexto de PGN.	

Migracion.1a.b.SIU Módulos

Submódulos Sistema Único de Información. Requerimientos asociados a submódulos.

versión 0.4

Identificación de submódulos del Sistema Único de Información (SUI) de la PGN.

Todos los sistemas de información del SUI deben seguir la directiva de separar a los componentes misionales de los utilitarios: el SUI de PGN estará constituidos por submódulos dispuestos en relación de utilitarios (que sirven) a los componentes misionales del SUI, ubicados en el centro en la diagrama.

Los submódulos del SUI, tal como están presentados, reúnen a las partes por el mismo rol en favor de la coherencia. Por ejemplo, los servicios de aplicación, en la imagen, contiene a todos aquellos utilitarios que prestan alguna utilidad momentánea al SUI migrado. Organizados así, estos submódulos utilitarios pueden ser intercambiados o ampliados sin perjuicio de los componentes misionales del SUI (centro del diagrama) gracias a las *interfaces de unión* en favor de la extensibilidad.

Las interfaces de unión indicadas arriba obligan a los submódulos a cumplir las exigencias de los componentes misionales del SUI.

Los submódulos identificados tienen los siguientes roles para el SUI migrado:

1. cc:Presentación
2. cc:Servicios de aplicación
3. cc:Portales y canales
4. cc:Administración y configuración
5. cc:Almacenamiento

Requerimientos Asociados a los Submódulos

La disposición de los módulos y submódulos presentada, denominada SUI Migración en adelante, facilita la focalización de los requerimientos encontrados en el levantamiento realizado en el actual proyecto. Así, por ejemplo, los requerimientos funcionales se encuentran concentrados en el submódulo de presentación (ver imagen).

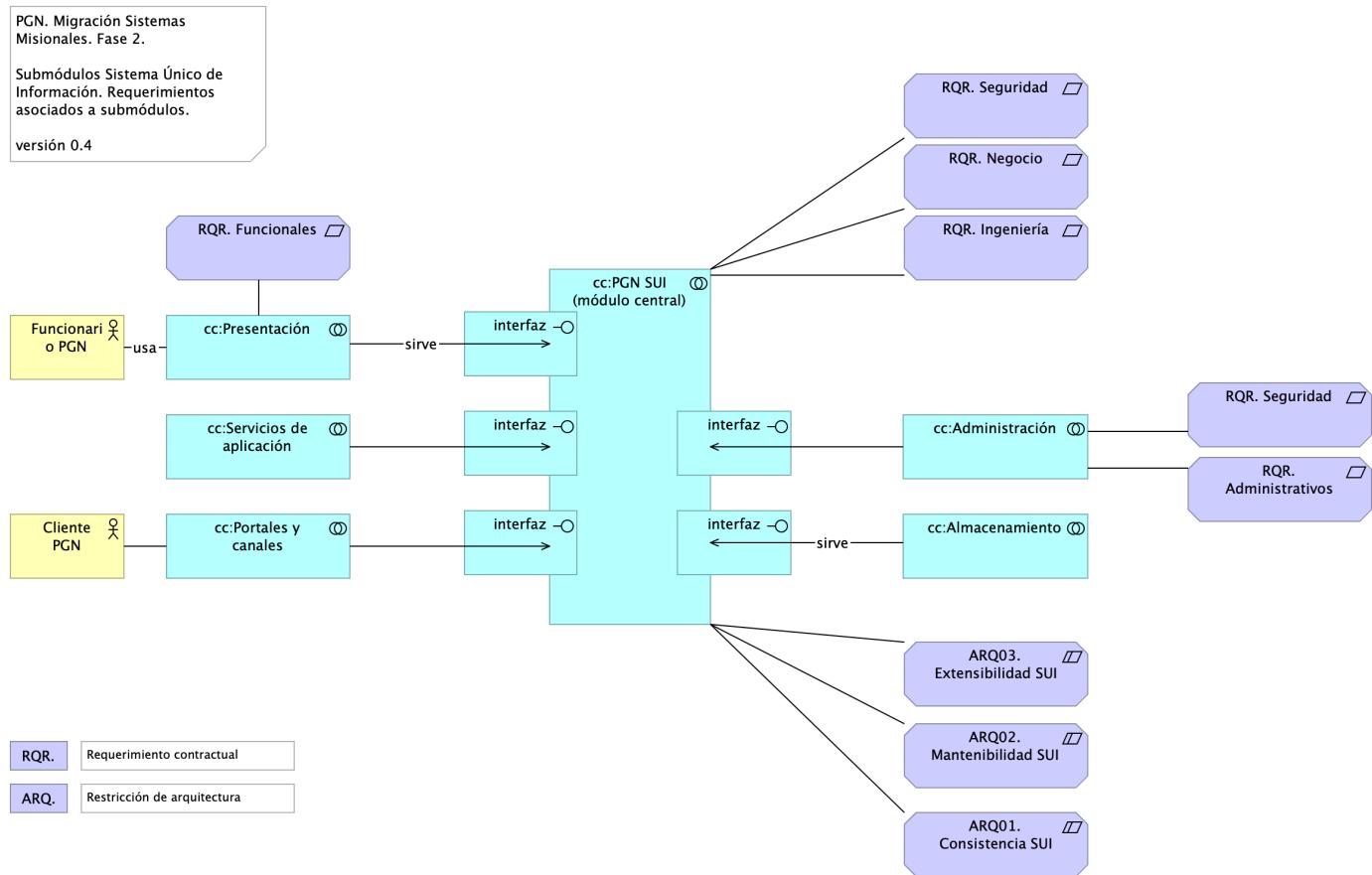


Imagen 30: Migracion.1a.b.SIU Módulos

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 28: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
--------	------	---------------	-----------

Nombre	Tipo	Documentación	Propiedad
ARQ01. Consistencia SUI	Constraint	<p>Unifica las entidades de negocio PGN, entre las que se incluyen a conciliaciones, publicaciones de relatoría, resoluciones, en artefactos reutilizables. Distinto de que estas entidades (y su lógica de negocio) estén dispersos entre los sistemas del SUI, estarán concentradas en un único artefacto correspondiente. Calidad sistemática: la consistencia persigue que el resultado de la lógica de negocio sea la misma entre los módulos del SUI migrado. Esto redundá a mantenibilidad y gestión: tiende a tener un solo punto de cambio y dificulta la transferencia de dependencias implícitas a otros procesos.</p>	
ARQ02. Mantenibilidad SUI	Constraint	<p>Evitar las dependencias transitivas de los módulos misionales del SUI a componentes y sistemas de terceros o submódulos no misionales. Calidad sistemática: la mantenibilidad por control de dependencias que optimiza el diseño. Migración SUI está dada por el control de cambios no programados sobre los componentes misionales del SUI (corrupción de componentes). Ver Patrón de Diseño Migración SUI, más adelante en el documento.</p>	
ARQ03. Extensibilidad SUI	Constraint	<p>Concentración de los componentes de negocio, misionales, del SUI protegidos de cambios provenientes de otros sistemas. Ver Patrón de Diseño Migración SUI, más adelante en el documento. Calidad sistemática: la extensibilidad que optimiza el diseño Migración SUI está dada por el intercambio de submódulos no misionales, como el gestor documental, sin afectación de los componentes misionales que este diseño protege.</p>	
Cliente PGN	Business Actor		
Funcionario PGN	Business Actor		
RQR. Administrativos	Requirement		
RQR. Funcionales	Requirement		
RQR. Ingeniería	Requirement		
RQR. Negocio	Requirement		
RQR. Seguridad	Requirement	Requerimientos de seguridad, SUI, Migración, en aspectos de comunicación, autenticación, autorización y (manejo de) sesiones.	
cc:Administración	Application Collaboration		
cc:Almacenamiento	Application Collaboration	Espacio de almacenamiento operativo y transaccional de un módulo central del SUI migrado.	
cc:PGN SUI (módulo central)	Application Collaboration	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN.	

Nombre	Tipo	Documentación	Propiedad
cc:Portales y canales	Application Collaboration	Submódulo de portales internos de la PGN a donde llega el SUI. Interfaz web que usa al SUI para llegar a direcciones y subdirecciones de la PGN. La plataforma principal de portales en este contexto es Sharepoint de Microsoft.	
cc:Presentación	Application Collaboration	Submódulo de presentación del SUI. interfaz gráfica, interfaz web visible a los usuarios clientes y funcionarios de la PGN.	
cc:Servicios de aplicación	Application Collaboration	Submódulo de servicios utilitarios que sirven al SUI. Servicios variados que cumplen roles facilitadores de las actividades misionales del SUI. Ejemplos de estos servicios son los de gestión documental, implementado por Doku en el contexto de PGN.	
interfaz	Application Interface		

Migracion.1b.1. SIU Módulos Componentes

PGN. Migración Sistemas Misionales. Fase 2.

Componentes internos de los submódulos Sistema Único de Información.

versión 0.45

Presentación de los componentes internos de los submódulos del sistema único de información migrado, SUI de PGN. Organización interna de los servicios y paquetes que integran cada submódulo del SUI. Todos los sistemas de información del SUI siguen esta directiva: estarán constituidos por submódulos dispuestos en relación de utilitarios (que sirven) a los componentes misionales del SUI, ubicados en el centro en la diagrama.

La organización de componentes de migración SUI facilita focalizar la selección de tecnologías. Los componentes internos y tecnologías elegidas son las siguientes

1. Presentación: Angular 11 (Web)
2. PGN SUI: API Transaccional (Node Js)
3. Administración: API Config (C#)
4. Persistencia: (SQL)

Los submódulos del SUI, tal como están presentados, reúnen a las partes que tienen el mismo rol en favor de la coherencia. Así mismo, estos pueden ser intercambiados o ampliados sin perjuicio del SUI gracias a las interfaces de unión (en favor de la extensibilidad).

Las interfaces de unión indicadas arriba obligan a los submódulos a cumplir las exigencias de los componentes misionales del SUI.

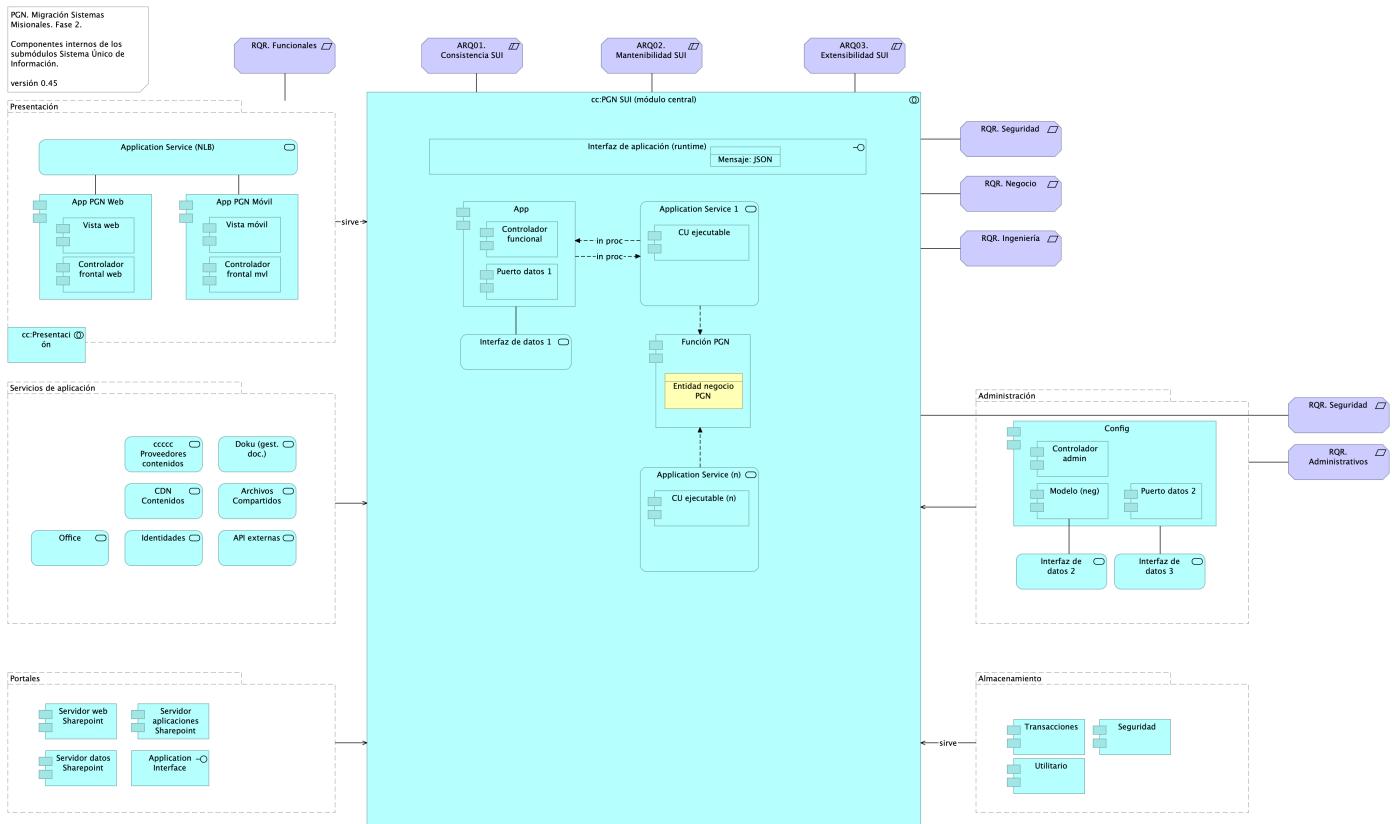


Imagen 31: Migracion.1b.1. SIU Módulos Componentes

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Nombre	Tipo	Documentación	Propiedad
API externas	Application Service		
ARQ01. Consistencia SUI	Constraint	<p>Unifica las entidades de negocio PGN, entre las que se incluyen a conciliaciones, publicaciones de relatorías, resoluciones, en artefactos reutilizables. Distinto de que estas entidades (y su lógica de negocio) estén dispersos entre los sistemas del SUI, estarán concentradas en un único artefacto correspondiente. Calidad sistemática: la consistencia persigue que el resultado de la lógica de negocio sea la misma entre los módulos del SUI migrado. Esto redundaría en una mayor mantenibilidad y gestión: tiende a tener un solo punto de cambio y dificulta la transferencia de dependencias implícitas a otros procesos.</p>	
ARQ02. Mantenibilidad SUI	Constraint	<p>Evitar las dependencias transitivas de los módulos misionales del SUI a componentes y sistemas de terceros o submódulos no misionales. Calidad sistemática: la mantenibilidad por control de dependencias que optimiza el diseño. La migración SUI está dada por el control de cambios no programados sobre los componentes misionales del SUI (corrupción de componentes). Ver Patrón de Diseño Migración SUI, más adelante en el documento.</p>	

Nombre	Tipo	Documentación	Propiedad
ARQ03. Extensibilidad SUI	Constraint	Concentración de los componentes de negocio, misionales, del SUI protegidos de cambios provenientes de otros sistemas. Ver Patrón de Diseño Migración SUI, más adelante en el documento. Calidad sistémica: la extensibilidad que optimiza el diseño Migración SUI está dada por el intercambio de submódulos no misionales, como el gestor documental, sin afectación de los componentes misionales que este diseño protege.	
Administración	Grouping		
Almacenamiento	Grouping		
App	Application Component		
App PGN Móvil	Application Component	A partir de los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la "Guía de desarrollo OWASP" y "OWAS Cheat Sheet, se realizarán pruebas de seguridad a partir del análisis de vulnerabilidades, y pruebas de Ethical Hacking.	

Protección de datos personales,

Los sistemas de información que recogen, procesan y almacenan información de los derechos de las personas se deben almacenar de forma adecuada, la información que pueda ser vulnerada puede generar obligaciones legales y éticas con respecto a la pérdida de información confidencial por parte de ciudadanos del país.

La información contenida en las bases de datos debe tener los mecanismos de cifrado que en otros apartados se han mencionado.

La legislación que hay que tener como referencia, ley 1581 de 2012. Decreto 1377 de 2013

La metodología empleada tendrá las siguientes fases:

- FASE DE RECONOCIMIENTO:

Se recolectará toda la información posible, usando diferentes técnicas como:

- o Recopilación de dominios/IPs/puertos/servicios
- o Recopilación de metadatos
- o Uso de Google Dorks.

- ANÁLISIS DE VULNERABILIDADES:

Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.

- EXPLOTACIÓN:

Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo:

- o Inyección de código
- o Inclusión de ficheros locales o remotos
- o Evasión de autenticación
- o Carencia de controles de autorización
- o Ejecución de comandos en el lado del servidor
- o Ataques tipo Cross Site Request Forgery
- o Control de errores
- o Gestión de sesiones
- o Fugas de información
- o Secuestros de sesión
- o Comprobación de las condiciones para realizar una denegación de servicio.

- POST EXPLOTACIÓN:

En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adicionales con el objetivo de comprobar la criticidad de esta.

No URL IP

1. https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz

| | | App PGN Web | Application Component | A partir de los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la "Guía de desarrollo OWASP" y "OWAS Cheat Sheet, se realizarán pruebas de seguridad a partir del análisis de vulnerabilidades, y pruebas de Ethical Hacking.

Los resultados permitirán identificar los requisitos de seguridad que los sistemas de información o servicios web deberán cumplir.

La metodología empleada tendrá las siguientes fases:

- FASE DE RECONOCIMIENTO:

Se recolectará toda la información posible, usando diferentes técnicas como:

- Recopilación de dominios/IPs/puertos/servicios
- Recopilación de metadatos
- Uso de Google Dorks.

- ANÁLISIS DE VULNERABILIDADES:

Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.

- EXPLOTACIÓN:

Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo:

- Inyección de código
- Inclusión de ficheros locales o remotos
- Evasión de autenticación
- Carencia de controles de autorización
- Ejecución de comandos en el lado del servidor
- Ataques tipo Cross Site Request Forgery
- Control de errores
- Gestión de sesiones
- Fugas de información
- Secuestros de sesión
- Comprobación de las condiciones para realizar una denegación de servicio.

- POST EXPLOTACIÓN:

En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adicionales con el objetivo de comprobar la criticidad de esta.

No URL IP

1. https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz
135.181.185.207

El Login deberá evidenciar el control de errores, al momento de realizar la validación deberá mensaje de error para el caso que se autentique con credenciales erradas. | | Application Interface | Application Interface | | | Application Service (NLB) | Application Service | | | Application Service (n) | Application Service | Implementación de un caso de uso de negocio, independiente y demostrable. Contiene a la unidad ejecutable del CU y a la entidad | | Application Service 1 | Application Service | Implementación de un caso de uso de negocio, independiente y demostrable. Contiene a la unidad ejecutable del CU y reutiliza (accede a) una entidad de negocio, que puede ser también una función PGN.

| | Archivos Compartidos | Application Service | | | CDN Contenidos | Application Service | | | CU ejecutable | Application Component | | | CU ejecutable (n) | Application Component | | | Config | Application Component | | | Controlador admin | Application Component | | | Controlador frontal mvl | Application Component | | | Controlador frontal web | Application Component | - Verificados los SSL, se recomienda adquirir SSL seguros, con entidades certificadoras.

Si se desea continuar con SSL de Let's Encrypt, se recomienda automatizar el proceso de actualización dado que al dejar estos en modo actualización manual es probable el olvido de esta actualización (Estos certificados se deben actualizar trimestralmente y no cuentan con las características de seguridad necesarias).

| | Controlador funcional | Application Component | | | Doku (gest. doc.) | Application Service | | | Entidad negocio PGN | Business Object | Representa un objeto de negocio del contexto de la entidad PGN,, por ejemplo: un decreto, una intervención, una conciliación.

| | Función PGN | Application Component | La unidad de cómputo que resulta en la aplicación de una regla de negocio.

| | Identidades | Application Service | | | Interfaz de aplicación (runtime) | Application Interface | Servidor web: Microsoft-IIS/10.0

Marco de Programación: ASP.NET

Huellas digitales identificadas:

Huella digital SHA-256 "FC:79:06:7E:F5:24:20:50:F1:C0:74:F7:85:56:B9:05:B7:33:A3:2D:44:A0:48"

Huella digital SHA1 "8C:48:BD:E2:F5:18:18:C3:85:96:68:44:2E:28:A0:68:08:2F:0A:BE"

| | Interfaz de datos 1 | Application Service | | | Interfaz de datos 2 | Application Service | | | Interfaz de datos 3 | Application Service | | |

Mensaje: JSON | Data Object | | | Modelo (neg) | Application Component | | | Office | Application Service | | | Portales | Grouping | Submódulo de portales internos de la PGN a donde llega el SUI. Interfaz web que usa al SUI para llegar a direcciones y subdirecciones de la PGN. La plataforma principal de portales en este contexto es Sharepoint de Microsoft.

| | Presentación | Grouping | Submódulo de presentación del SUI. interfaz gráfica, interfaz web visible a los usuarios clientes y funcionarios de la PGN.

| | Puerto datos 1 | Application Component | | | Puerto datos 2 | Application Component | | | RQR. Administrativos | Requirement | | | RQR.

Funcionales | Requirement | | | RQR. Ingeniería | Requirement | | | RQR. Negocio | Requirement | | | RQR. Seguridad | Requirement |

Requerimientos de seguridad, SUI, Migración, en aspectos de comunicación, autenticación, autorización y (manejo de) sesiones.

| | Seguridad | Application Component | | | Servicios de aplicación | Grouping | Submódulo de servicios utilitarios que sirven al SUI. Servicios variados que cumplen roles facilitadores de las actividades misionales del SUI. Ejemplos de estos servicios son los de gestión documental, implementado por Doku en el contexto de PGN.

| | Servidor aplicaciones Sharepoint | Application Component | | | Servidor datos Sharepoint | Application Component | | | Servidor web Sharepoint | Application Component | | | Transacciones | Application Component | | | Utilitario | Application Component | | | Vista móvil | Application Component | | | Vista web | Application Component | - Verificados los SSL, se recomienda adquirir SSL seguros, con entidades certificadoras.

Si se desea continuar con SSL de Let's Encrypt, se recomienda automatizar el proceso de actualización dado que al dejar estos en modo actualización manual es probable el olvido de esta actualización (Estos certificados se deben actualizar trimestralmente y no cuentan con las características de seguridad necesarias).

4. SERVICIOS IDENTIFICADOS:

Servidor web: Microsoft-IIS/10.0

Marco de Programación: ASP.NET

Huellas digitales identificadas:

Huella digital SHA-256 "FC:79:06:7E:F5:24:20:50:F1:C0:74:F7:85:56:B9:05:B7:33:A3:2D:44:A0:48"

Huella digital SHA1 "8C:48:BD:E2:F5:18:18:C3:85:96:68:44:2E:28:A0:68:08:2F:0A:BE"

| | cc:PGN SUI (módulo central) | Application Collaboration | Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN.

| | cc:Presentación | Application Collaboration | Submódulo de presentación del SUI. interfaz gráfica, interfaz web visible a los usuarios clientes y funcionarios de la PGN. | | cccc Proveedores contenidos | Application Service | | |

Table: Elementos de la vista. {#tbl:tblelement-Migracion.1b.1.SIU Módulos Componentes-id}

Migracion.1b.2. SIU Módulos Componentes. Brecha

PGN. Migración Sistemas Misionales. Fase 2.

Componentes internos de los submódulos Sistema Único de Información.

versión 0.45

Los elementos resaltados indican las extensiones a la arquitectura por concepto de Fase II del proyecto de migración SUI.

Los componentes internos incorporados en la arquitectura tienen el propósito de implementar los casos de uso (CU) de cada módulo construido con esta organización (vista anterior). En la imagen los CU son expuestos por los servicios de aplicación, y estos a su vez, usan funciones de negocio (impulsadas por la plataforma de Lappiz).

Todos los sistemas de información del SUI siguen esta directiva: estarán constituidos por submódulos dispuestos en relación de utilitarios (que sirven) a los componentes misionales del SUI, ubicados en el centro en la diagrama.

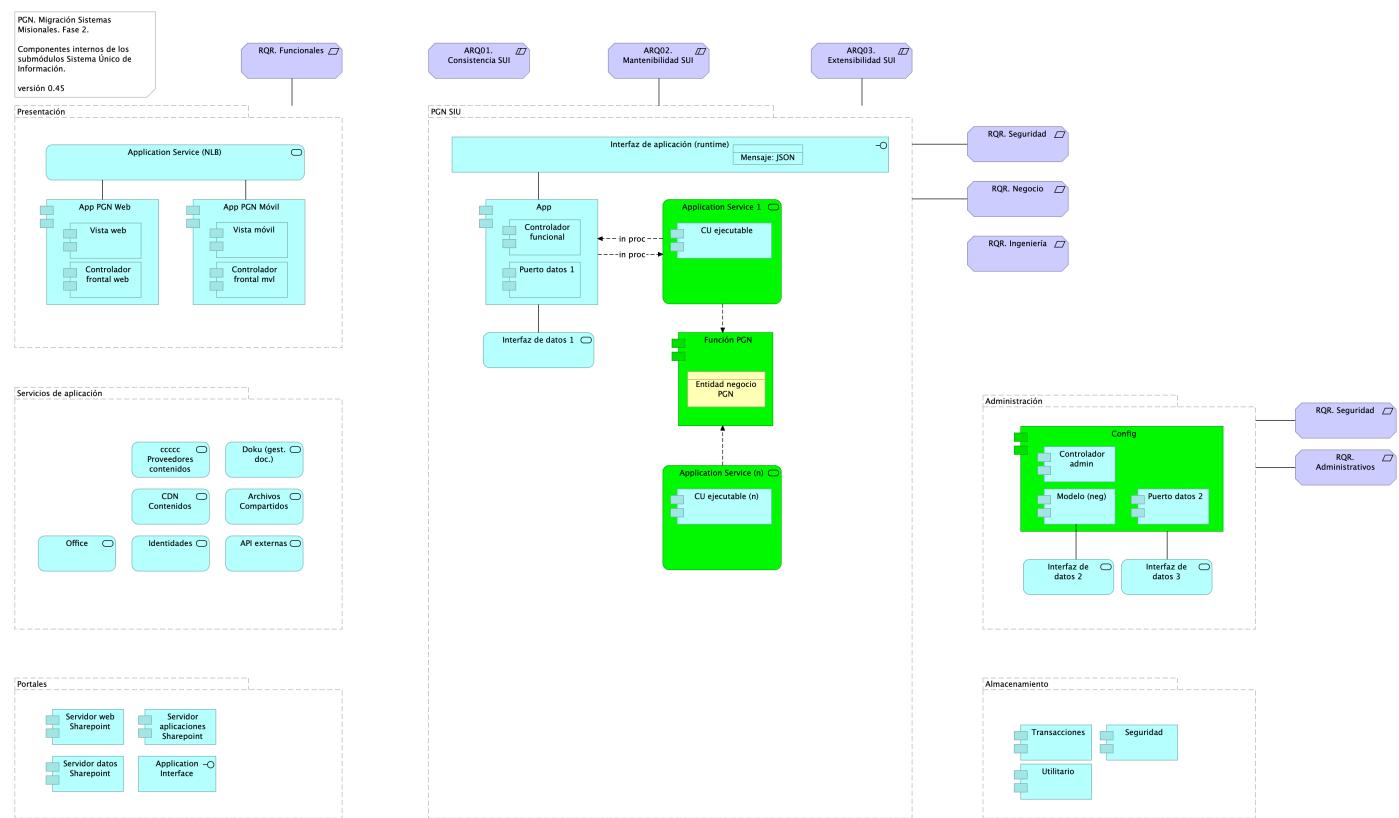


Imagen 32: Migracion.1b.2. SIU Módulos Componentes. Brecha

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Nombre	Tipo	Documentación	Propiedad
API externas	Application Service		

Nombre	Tipo	Documentación	Propiedad
ARQ01. Consistencia SUI	Constraint	Unifica las entidades de negocio PGN, entre las que se incluyen a conciliaciones, publicaciones de relatoría, resoluciones, en artefactos reutilizables. Distinto de que estas entidades (y su lógica de negocio) estén dispersos entre los sistemas del SUI, estarán concentradas en un único artefacto correspondiente. Calidad sistemática: la consistencia persigue que el resultado de la lógica de negocio sea la misma entre los módulos del SUI migrado. Esto redundá a mantenibilidad y gestión: tiende a tener un solo punto de cambio y dificulta la transferencia de dependencias implícitas a otros procesos.	
ARQ02. Mantenibilidad SUI	Constraint	Evitar las dependencias transitivas de los módulos misionales del SUI a componentes y sistemas de terceros o submódulos no misionales. Calidad sistemática: la mantenibilidad por control de dependencias que optimiza el diseño. Migración SUI está dada por el control de cambios no programados sobre los componentes misionales del SUI (corrupción de componentes). Ver Patrón de Diseño Migración SUI, más adelante en el documento.	
ARQ03. Extensibilidad SUI	Constraint	Concentración de los componentes de negocio, misionales, del SUI protegidos de cambios provenientes de otros sistemas. Ver Patrón de Diseño Migración SUI, más adelante en el documento. Calidad sistemática: la extensibilidad que optimiza el diseño Migración SUI está dada por el intercambio de submódulos no misionales, como el gestor documental, sin afectación de los componentes misionales que este diseño protege.	
Administración	Grouping		
Almacenamiento	Grouping		
App	Application Component		
App PGN Móvil	Application Component	A partir de los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la "Guía de desarrollo OWASP" y "OWAS Cheat Sheet, se realizarán pruebas de seguridad a partir del análisis de vulnerabilidades, y pruebas de Ethical Hacking.	

Protección de datos personales,

Los sistemas de información que recogen, procesan y almacenan información de los derechos de las personas se deben almacenar de forma adecuada, la información que pueda ser vulnerada puede generar obligaciones legales y éticas con respecto a la pérdida de información confidencial por parte de ciudadanos del país.

La información contenida en las bases de datos debe tener los mecanismos de cifrado que en otros apartados se han mencionado. La legislación que hay que tener como referencia, ley 1581 de 2012. Decreto 1377 de 2013

La metodología empleada tendrá las siguientes fases:

- FASE DE RECONOCIMIENTO:

Se recolectará toda la información posible, usando diferentes técnicas como:
o Recopilación de dominios/IPs/puertos/servicios

- o Recopilación de metadatos
- o Uso de Google Dorks.

• ANÁLISIS DE VULNERABILIDADES:

Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.

• EXPLOTACIÓN:

- Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo:
- o Inyección de código
- o Inclusión de ficheros locales o remotos
- o Evasión de autenticación
- o Carencia de controles de autorización
- o Ejecución de comandos en el lado del servidor
- o Ataques tipo Cross Site Request Forgery
- o Control de errores
- o Gestión de sesiones
- o Fugas de información
- o Secuestros de sesión
- o Comprobación de las condiciones para realizar una denegación de servicio.

• POST EXPLOTACIÓN:

En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adicionales con el objetivo de comprobar la criticidad de esta.

No URL IP

1. https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz
135.181.185.207

| | | App PGN Web | Application Component | A partir de los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la "Guía de desarrollo OWASP" y "OWAS Cheat Sheet", se realizarán pruebas de seguridad a partir del análisis de vulnerabilidades, y pruebas de Ethical Hacking.

Los resultados permitirán identificar los requisitos de seguridad que los sistemas de información o servicios web deberán cumplir.

La metodología empleada tendrá las siguientes fases:

• FASE DE RECONOCIMIENTO:

Se recolectará toda la información posible, usando diferentes técnicas como:

- o Recopilación de dominios/IPs/puertos/servicios
- o Recopilación de metadatos
- o Uso de Google Dorks.

• ANÁLISIS DE VULNERABILIDADES:

Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.

• EXPLOTACIÓN:

- Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo:

- o Inyección de código
- o Inclusión de ficheros locales o remotos
- o Evasión de autenticación
- o Carencia de controles de autorización
- o Ejecución de comandos en el lado del servidor
- o Ataques tipo Cross Site Request Forgery
- o Control de errores
- o Gestión de sesiones
- o Fugas de información
- o Secuestros de sesión
- o Comprobación de las condiciones para realizar una denegación de servicio.

• POST EXPLOTACIÓN:

En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adicionales con el objetivo de comprobar la criticidad de esta.

No URL IP

1. https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz
135.181.185.207

El Login deberá evidenciar el control de errores, al momento de realizar la validación deberá mensaje de error para el caso que se autentique con credenciales erradas. | | | Application Interface | Application Interface | | | Application Service (NLB) | Application Service | | | Application Service (n) | Application Service | Implementación de un caso de uso de negocio, independiente y demostrable. Contiene a la unidad ejecutable del CU y a la entidad | | | Application Service 1 | Application Service | Implementación de un caso de uso de negocio, independiente y demostrable. Contiene a la unidad ejecutable del CU y reutiliza (accede a) una entidad de negocio, que puede ser también una función PGN.

| | | Archivos Compartidos | Application Service | | | CDN Contenidos | Application Service | | | CU ejecutable | Application Component | | | CU ejecutable (n) | Application Component | | | Config | Application Component | | | Controlador admin | Application Component | | | Controlador frontal mvl | Application Component | | | Controlador frontal web | Application Component | - Verificados los SSL, se recomienda adquirir SSL seguros, con entidades certificadoras.

Si se desea continuar con SSL de Let's Encrypt, se recomienda automatizar el proceso de actualización dado que al dejar estos en modo actualización manual es probable el olvido de esta actualización (Estos certificados se deben actualizar trimestralmente y no cuentan con las características de

seguridad necesarias.

| | | Controlador funcional | Application Component | | | Doku (gest. doc.) | Application Service | | | Entidad negocio PGN | Business Object |
Represents a business object within the context of the entity PGN, for example: a decree, an intervention, a reconciliation.

| | | Función PGN | Application Component | La unidad de cómputo que resulta en la aplicación de una regla de negocio.

| | | Identidades | Application Service | | | Interfaz de aplicación (runtime) | Application Interface | Servidor web: Microsoft-IIS/10.0

Marco de Programación: ASP.NET

Huellas digitales identificadas:

Huella digital SHA-256 "FC:79:06:7E:F5:24:20:50:F1:C0:74:F7:85:56:B9:05:B7:33:A3:2D:44:A0:48"

Huella digital SHA1 "8C:48:BD:E2:F5:18:18:C3:85:96:68:44:2E:28:A0:68:08:2F:0A:BE"

| | | Interfaz de datos 1 | Application Service | | | Interfaz de datos 2 | Application Service | | | Interfaz de datos 3 | Application Service | | |

Mensaje: JSON | Data Object | | | Modelo (neg) | Application Component | | | Office | Application Service | | | PGN SIU | Grouping | El objetivo principal de la arquitectura del SUI de la migración es la centralización de los conceptos misionales: concentrar los conceptos misionales en componentes aislados; dejar por fuera de estos componentes misionales todo lo distintos a la misionalidad de la PGN.

Los objetivos secundarios de esta arquitectura SUI de la migración son flexibilidad y extensibilidad. Dichos objetivos son independientes. Es decir, estos pueden ser maximizados sin conflicto entre ellos.

| | | Portales | Grouping | Submódulo de portales internos de la PGN a donde llega el SUI. Interfaz web que usa al SUI para llegar a direcciones y subdirecciones de la PGN. La plataforma principal de portales en este contexto es Sharepoint de Microsoft.

| | | Presentación | Grouping | Submódulo de presentación del SUI. interfaz gráfica, interfaz web visible a los usuarios clientes y funcionarios de la PGN.

| | | Puerto datos 1 | Application Component | | | Puerto datos 2 | Application Component | | | RQR. Administrativos | Requirement | | | RQR. Funcionales | Requirement | | | RQR. Ingeniería | Requirement | | | RQR. Negocio | Requirement | | | RQR. Seguridad | Requirement | Requerimientos de seguridad, SUI, Migración, en aspectos de comunicación, autenticación, autorización y (manejo de) sesiones.

| | | Seguridad | Application Component | | | Servicios de aplicación | Grouping | Submódulo de servicios utilitarios que sirven al SUI. Servicios variados que cumplen roles facilitadores de las actividades misionales del SUI. Ejemplos de estos servicios son los de gestión documental, implementado por Doku en el contexto de PGN.

| | | Servidor aplicaciones Sharepoint | Application Component | | | Servidor datos Sharepoint | Application Component | | | Servidor web Sharepoint | Application Component | | | Transacciones | Application Component | | | Utilitario | Application Component | | | Vista móvil | Application Component | | | Vista web | Application Component | - Verificados los SSL, se recomienda adquirir SSL seguros, con entidades certificadoras.

Si se desea continuar con SSL de Let's Encrypt, se recomienda automatizar el proceso de actualización dado que al dejar estos en modo actualización manual es probable el olvido de esta actualización (Estos certificados se deben actualizar trimestralmente y no cuentan con las características de seguridad necesarias.

4. SERVICIOS IDENTIFICADOS:

Servidor web: Microsoft-IIS/10.0

Marco de Programación: ASP.NET

Huellas digitales identificadas:

Huella digital SHA-256 "FC:79:06:7E:F5:24:20:50:F1:C0:74:F7:85:56:B9:05:B7:33:A3:2D:44:A0:48"

Huella digital SHA1 "8C:48:BD:E2:F5:18:18:C3:85:96:68:44:2E:28:A0:68:08:2F:0A:BE"

| | | ccccc Proveedores contenidos | Application Service | | |

Table: Elementos de la vista. {#tbl:tblElement-Migracion.1b.2.SIU Módulos Componentes.Brecha-id}

Migracion.1c.SIU Modulos Colaboración

PGN. Migración Sistemas Misionales. Fase 2.

Patrones de comunicación y colaboración. a) entre módulos central SUI de PGN. b) colaboración intraproceso. Puertos, adaptadores y API.

versión 0.4.1

Patrón de Distribución y Colaboración estándar para el SUI.

La colaboración y comunicación de los componentes internos del SUI (grupo PFN SUI, en el diagrama) está mediada por interfaces. Estas son provistas por el grupo de componentes misionales, PGN SUI, hacia los submódulos externos. La intención es mantener reducido y controlado el número de interfaces.

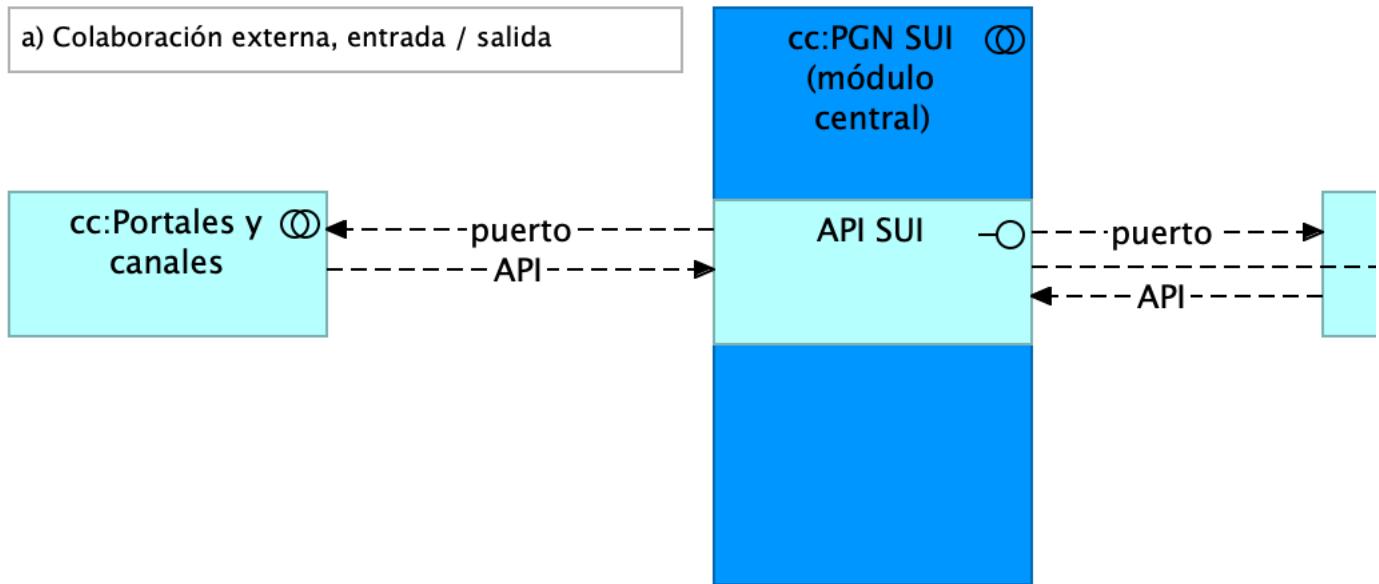
La colaboración entre el SUI Migración con sistemas externos puede darse mediante API de comunicación (o buses de datos empresarial que ya disponga la PGN), sin perjuicio del patrón de comunicación estar descrito en el diagrama.

Los únicos elementos para la comunicación (e integración) son los indicados en la vista actual. En este diseño no considera tipos de comunicación mediante mesajería, datos, ni

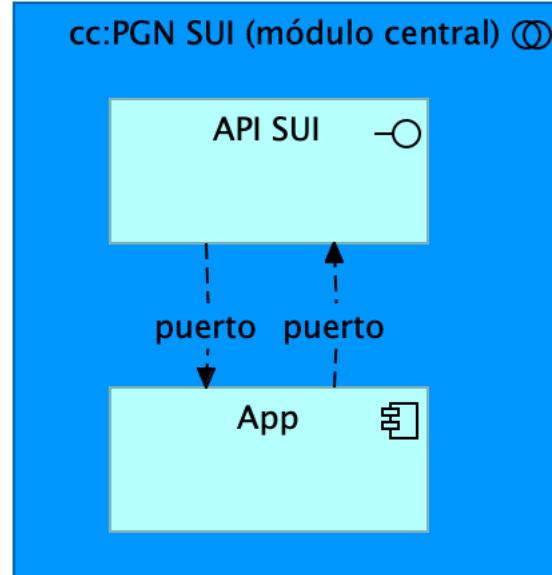
PGN. Migración Sistemas Misionales. Fase 2.

**Patrones de comunicación y colaboración. a)
entre módulos central SUI de PGN. b)
colaboración intraproceso. Puertos, adaptadores
y API.**

a) Colaboración externa, entrada / salida



b) Colaboración intraproceso, entrada / salida



	Módulos centrales SIU migrados
	Submódulos SIU migrados

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 29: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
API SUI	Application Interface	API de representación del módulo. Centralización de la comunicación con otros módulos del SUI migrado.	
API SUI 2	Application Interface	API de representación del módulo. Centralización de la comunicación con otros módulos del SUI migrado.	
App	Application Component		
cc:Almacenamiento	Application Collaboration	Espacio de almacenamiento operativo y transaccional de un módulo central del SUI migrado.	
cc:PGN SUI (módulo central)	Application Collaboration	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN.	
cc:PGN SUI (módulo central) 2	Application Collaboration	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN.	
cc:Portales y canales	Application Collaboration	Submódulo de portales internos de la PGN a donde llega el SUI. Interfaz web que usa al SUI para llegar a direcciones y subdirecciones de la PGN. La plataforma principal de portales en este contexto es Sharepoint de Microsoft.	

Migracion.2. datos

PGN. Migración Sistemas Misionales. Fase 2.

Modelo de acceso y procesamiento de datos de negocio. Módulos Sistema Único de Información.

versión 0.1

Modelo de acceso y procesamiento a datos de negocio del SUI. Presentamos la organización de los ítems de datos de negocio necesarios para que los módulos del SUI puedan recolectar, procesar, integrar y almacenarlos de forma organizada y escalable.

Mediante esta organización, los datos de negocio son transportados desde sus respectivas fuentes mediante interfaces (por principio de extensión y mantenibilidad). Los datos externos, entendidos como los de otros proveedores, son obtenidos mediante un intermediario: el bus de datos del SUI.

Consideramos tres tipos datos: datos transaccionales, históricos y externos, y presentamos una manera distinta de tratarlos y transportarlos.

PGN. Migración Sistemas Misionales.
Fase 2.

Modelo de acceso y procesamiento
de datos de negocio. Módulos
Sistema Único de Información.

versión 0.1

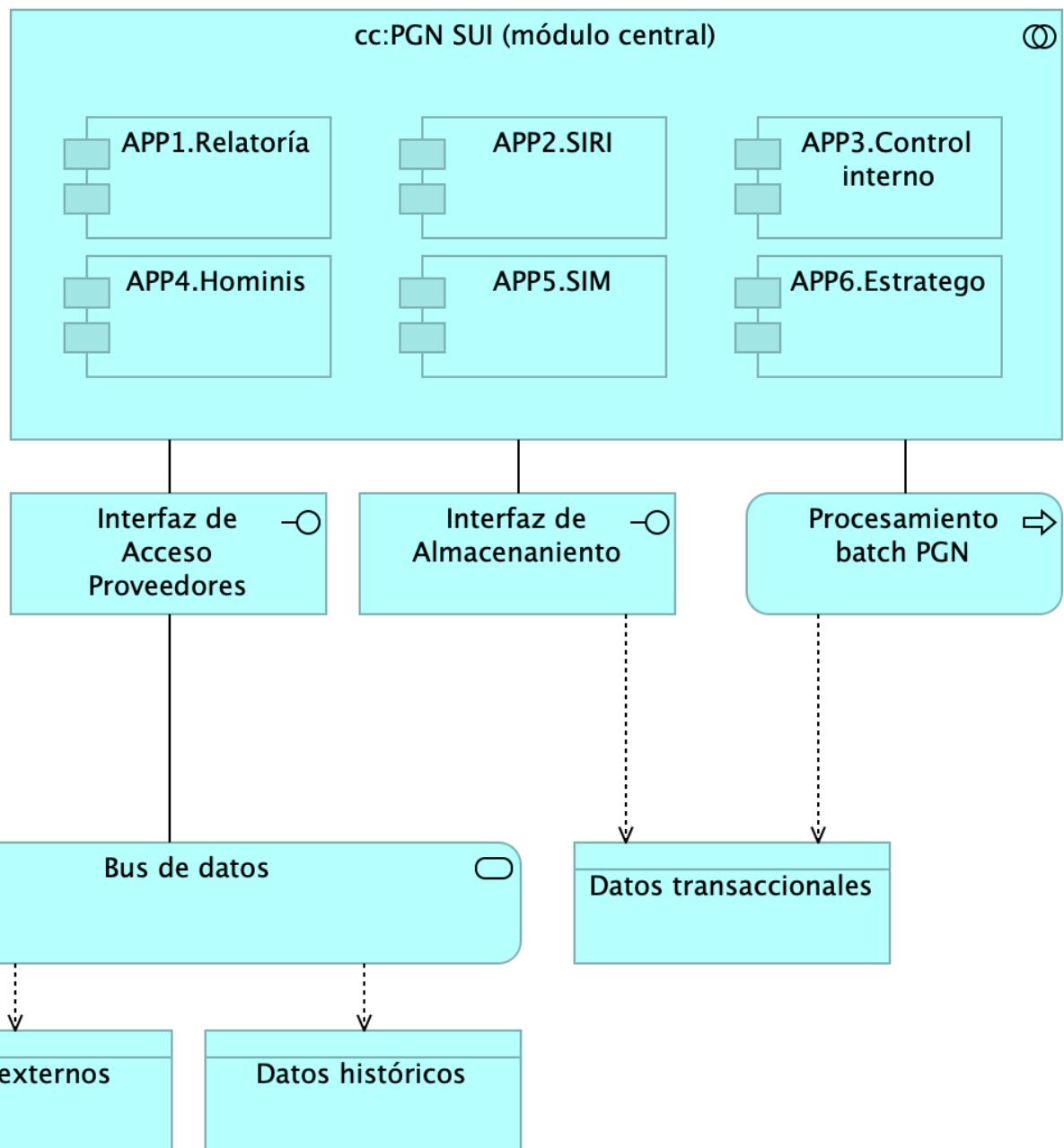


Imagen 33: Migracion.2. datos

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 30: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
--------	------	---------------	-----------

Nombre	Tipo	Documentación	Propiedad
APP1.Relatoría	Application Component	Módulo del SUI. Relatoría pública. Publicación de información de referencia para funcionarios y personas naturales, clientes de la PGN.	
APP2.SIRI	Application Component		
APP3.Control interno	Application Component		
APP4.Hominis	Application Component	Módulo del SUI. Gestión de capital humano, funcionarios y cargos de representación y libre remoción de la PGN.	
APP5.SIM	Application Component		
APP6.Estratego	Application Component		
Bus de datos	Application Service	El patrón de bus de datos tiene el rol de unir y referir a los datos externos al SUI de tal manera que hace transparente la localización y el formato de este tipo de datos.	
Datos externos	Data Object		
Datos históricos	Data Object		
Datos transaccionales	Data Object		
Interfaz de Acceso Proveedores	Application Interface	Interfaz de acceso a los tipos de datos externos al SUI.	
Interfaz de Almacenamiento	Application Interface	Interfaz de acceso a los repositorio, base de datos relacionales y no jerárquicas. Tipos de datos transaccionales, internos, del SUI.	
Procesamiento batch PGN	Application Process	Los procesos de lotes, que requieren volúmenes de datos altos, deben hacer parte de la arquitectura de datos del SUI.	
cc:PGN SUI (módulo central)	Application Collaboration	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN.	

Migracion.2a. datos Hominis

PGN. Migración Sistemas Misionales. Fase 2.

Entidades de datos de negocio. Submódulos Sistema Único de Información. Hominis

versión 0.1

Identificación de entidades de datos de negocio relacionadas al módulo de gestión de capital del SUI, Hominis.

Estas entidades de datos de negocio son las que llamamos los tipos de datos internos del SUI y deben ser consideradas para la creación de las API de manejo del ciclo de vida de los datos de este módulo.

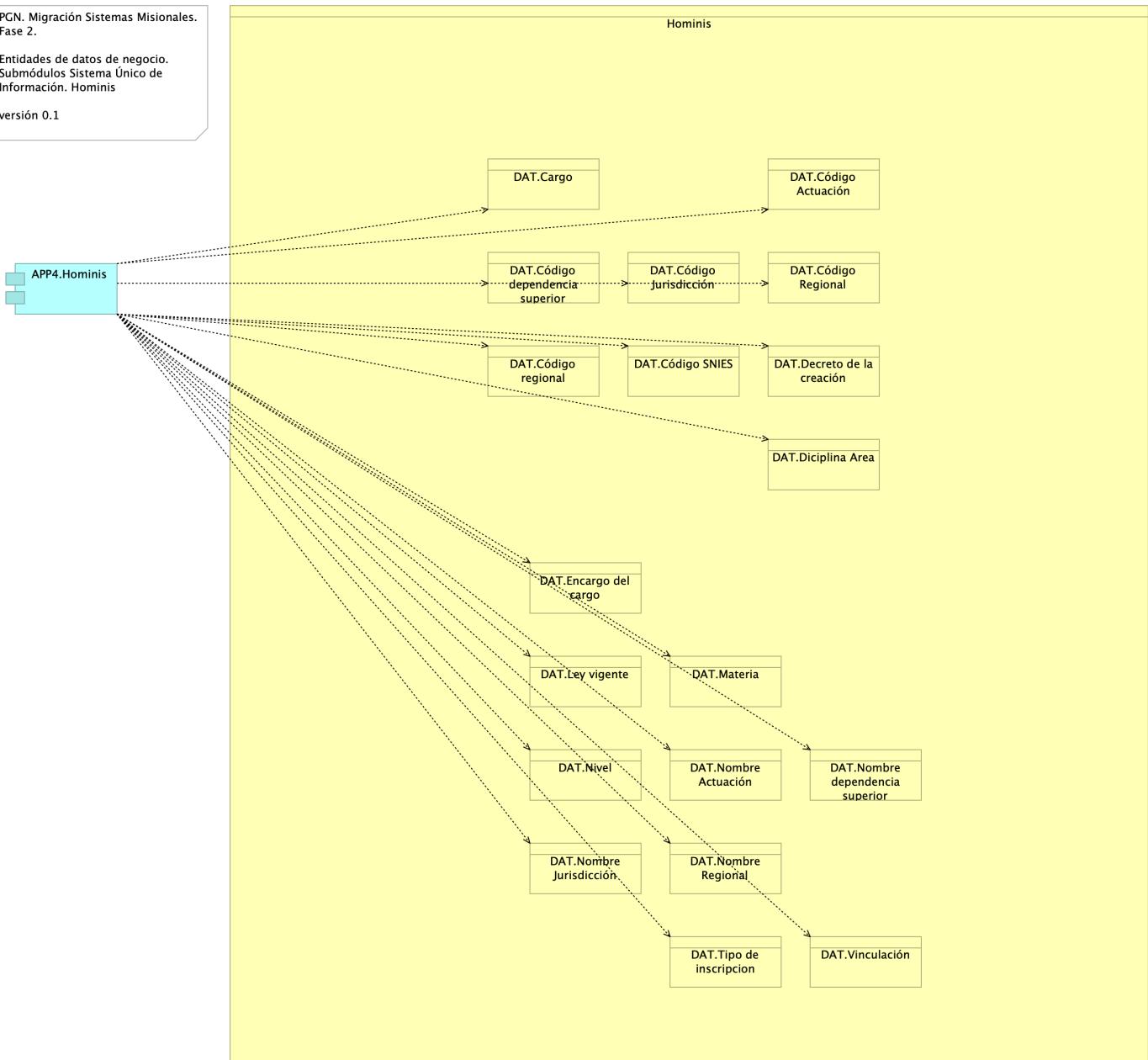


Imagen 34: Migracion.2a. datos Hominis

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 31: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
APP4.Hominis	Application Component	Módulo del SUI. Gestión de capital humano, funcionarios y cargos de representación y libre remoción de la PGN.	
DAT.Cargo	Business Object		
DAT.Código Actuación	Business Object		
DAT.Código Jurisdicción	Business Object		
DAT.Código Regional	Business Object		
DAT.Código SNIES	Business Object		
DAT.Código dependencia superior	Business Object		
DAT.Código regional	Business Object		
DAT.Decreto de la creación	Business Object		
DAT.Disciplina Area	Business Object		
DAT.Encargo del cargo	Business Object		

Nombre	Tipo	Documentación	Propiedad
DAT.Ley vigente	Business Object		
DAT.Materia	Business Object		
DAT.Nivel	Business Object		
DAT.Nombre Actuación	Business Object		
DAT.Nombre Jurisdicción	Business Object		
DAT.Nombre Regional	Business Object		
DAT.Nombre dependencia superior	Business Object		
DAT.Tipo de inscripción	Business Object		
DAT.Vinculación	Business Object		
Hominis	Business Object	Entidades de datos de negocio de capital humano de la PGN. Sistema de información Hombini.	

Migracion.2d. datos Control Interno

PGN. Migración Sistemas Misionales. Fase 2.

Entidades de datos de negocio. Submódulos Sistema Único de Información. Control Interno

versión 0.1

Identificación de entidades de datos de negocio relacionadas al módulo de seguimiento del desempeño de la PGN del SUI, Control Interno.

Estas entidades de datos de negocio son los que llamamos los tipos de datos internos del SUI y deben ser consideradas para la creación de las API de manejo del ciclo de vida de los datos de este módulo.

PGN. Migración Sistemas Misionales. Fase 2.

Entidades de datos de negocio.
Submódulos Sistema Único de
Información. Control Interno

versión 0.1

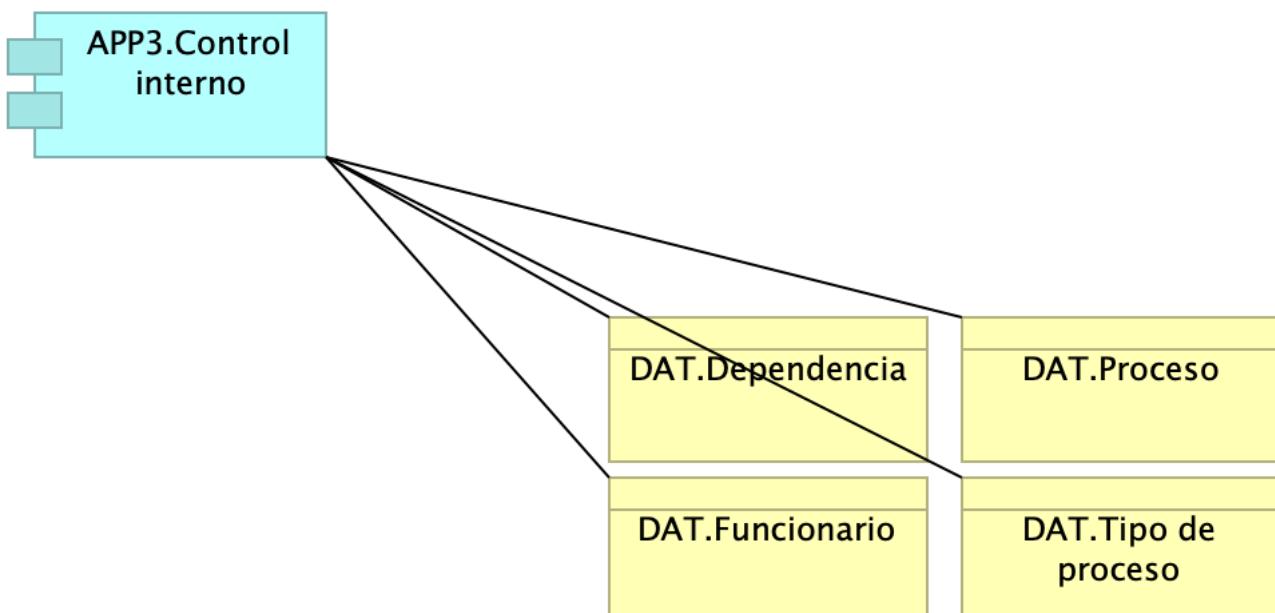


Imagen 35: Migracion.2d. datos Control Interno

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 32: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
APP3.Control interno	Application Component		
DAT.Dependencia	Business Object		
DAT.Funcionario	Business Object		
DAT.Proceso	Business Object		
DAT.Tipo de proceso	Business Object		

Migracion.2d. datos SIM

PGN. Migración Sistemas Misionales. Fase 2.

Entidades de datos de negocio. Submódulos Sistema Único de Información. SIM

versión 0.1

Identificación de entidades de datos de negocio relacionadas al módulo de SUI, SIM.

Estas entidades de datos de negocio son los que llamamos los tipos de datos internos del SUI y deben ser consideradas para la creación de las API de manejo del ciclo de vida de los datos de este módulo.

**PGN. Migración Sistemas Misionales.
Fase 2.**

**Entidades de datos de negocio.
Submódulos Sistema Único de
Información. SIM**

versión 0.1

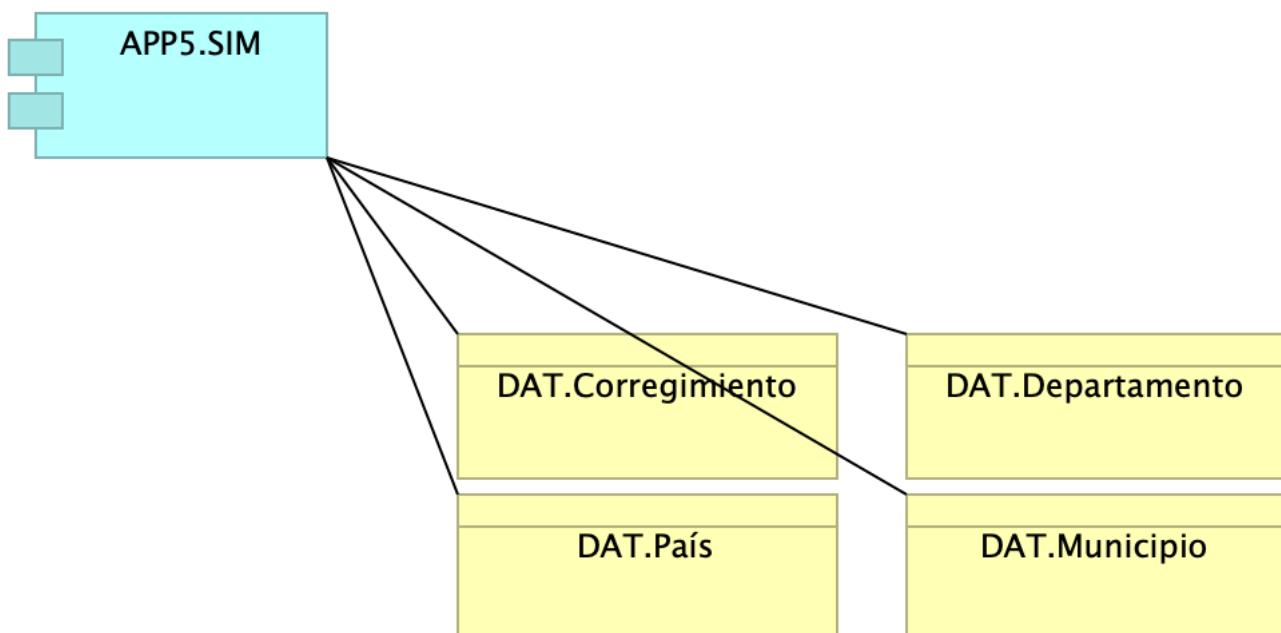


Imagen 36: Migracion.2d. datos SIM

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 33: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
APP5.SIM	Application Component		
DAT.Corregimiento	Business Object		
DAT.Departamento	Business Object		
DAT.Municipio	Business Object		
DAT.País	Business Object		

Migracion.2d. datos SIRI

PGN. Migración Sistemas Misionales. Fase 2.

Entidades de datos de negocio. Submódulos Sistema Único de Información. SIRI

versión 0.1

Identificación de entidades de datos de negocio relacionadas al módulo del SUI, SIRI.

Estas entidades de datos de negocio son los que llamamos los tipos de datos internos del SUI y deben ser consideradas para la creación de las API de manejo del ciclo de vida de los datos de este módulo.

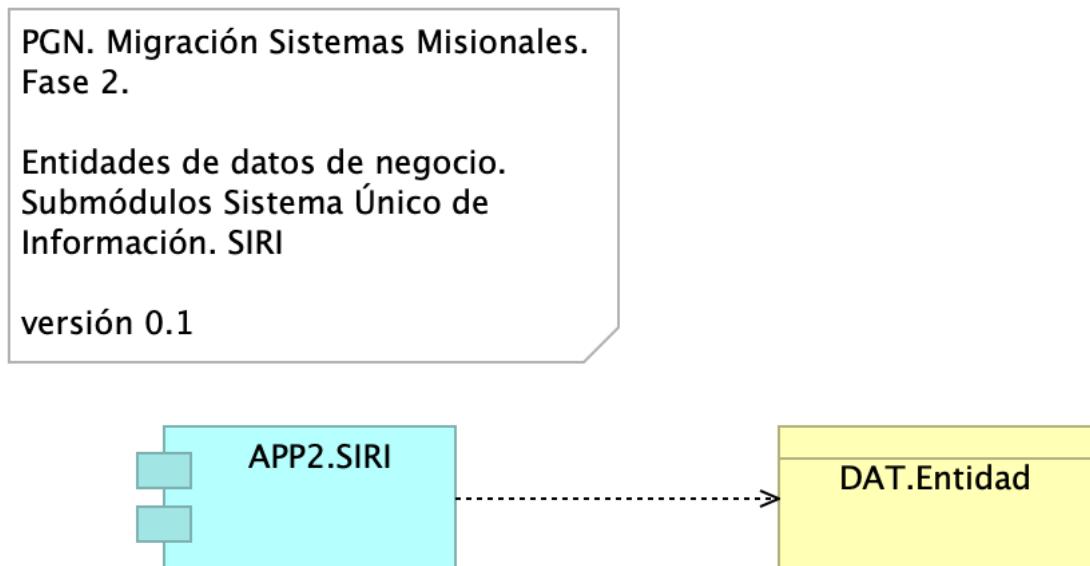


Imagen 37: Migracion.2d. datos SIRI

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 34: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
APP2.SIRI	Application Component		
DAT.Entidad	Business Object		

Migracion.3. Infraestructura

PGN. Migración Sistemas Misionales. Fase 2.

Diseño de infraestructura. Módulos Central Sistema Único de Información, SIU de PGN.

versión 0.1.1

Identificación de entidades de datos de negocio relacionadas al módulo del SUI, SIRI.

Estas entidades de datos de negocio son los que llamamos los tipos de datos internos del SUI y deben ser consideradas para la creación de las API de manejo del ciclo de vida de los datos de este módulo.

PGN. Migración Sistemas Misionales. Fase 2.

Diseño de infraestructura. Módulos
Central Sistema Único de
Información, SIU de PGN.

versión 0.1.1

Imagen 38: Migracion.3. Infraestructura

Fuente: *Repositorio arquitectura Mi Mutual (2023)*

Catálogo de Elementos

Tabla 35: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
--------	------	---------------	-----------

Migracion.4. CI

PGN. Migración Sistemas Misionales. Fase 2.

Patrón de integración/entrega continuo. Módulos Central Sistema Único de Información, SIU de PGN.

versión 0.1.1

Descripción de las cadenas de integración y despliegue continuo de a) submódulos (aplicaciones web, por ejemplo) del SIU Migrado, 2023; e integración y despliegue continuo de los meodulos central del SIU Migrado, 2023.

Las cadenas están separadas por tecnologías y plataformas distintas; son independientes y no presentan interbloqueos en cuanto a su ejecución. Pero, requieren administración integral.

Los trabajo de despliegue requieren las configuraciones de las cadenas y tareas de conexión tanto a los ambientes productivos y desarrollo.

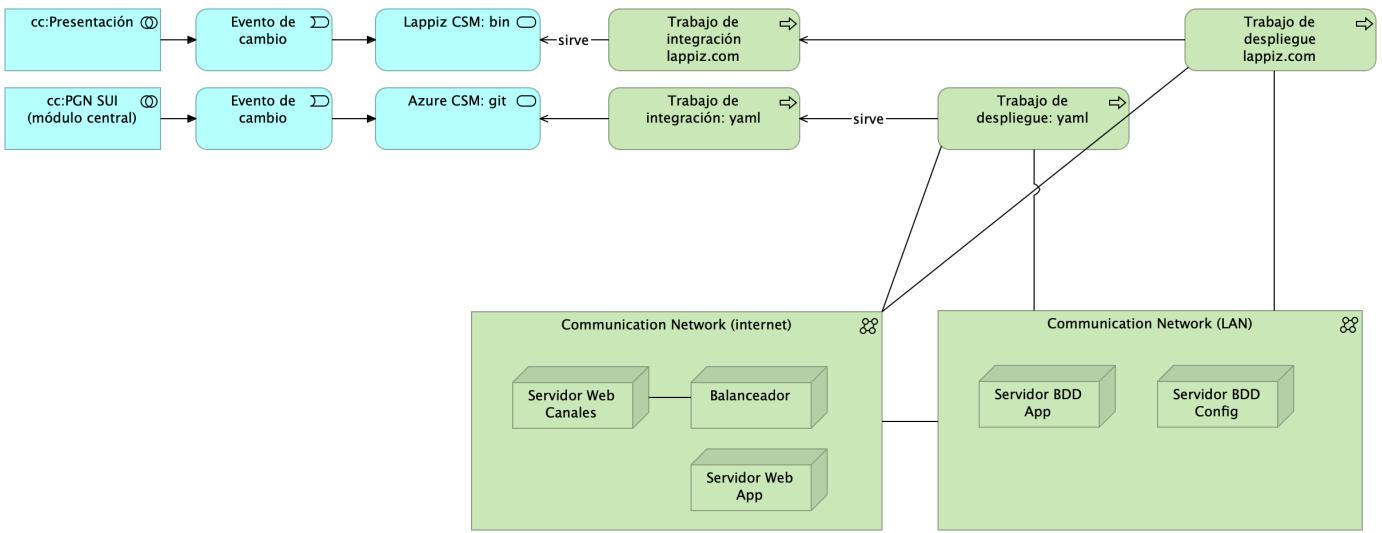


Imagen 39: Migracion.4. CI

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 36: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
Azure CSM: git	Application Service		
Balanceador	Node		
Communication Network (LAN)	Communication Network		
Communication Network (internet)	Communication Network		
Evento de cambio	Application Event		
Evento de cambio	Application Event		
Lappiz CSM: bin	Application Service		
Servidor BDD App	Node	Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz Discos SO C: 126 GB, Backup E: 511 GB, SQL Data F: 510 GB, SQL Log G: 510 GB, TempDB H: 63.6 GB.	
Servidor BDD Config	Node	Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz Discos SO C: 80 GB, Backup E: 250 GB, SQL Data F: 250 GB, SQL Log G: 250 GB, TempDB H: 30 GB.	
Servidor Web App	Node	Windows Server 2019 Standard o Datacenter x64. Nombre físico. IP LAN. IP Pública. Windows Server 2019 Standard or Datacenter x64. RAM 8 GB. CPU 64 Bits. 4 Cores de 2 Ghz. Discos SO C: 126 GB. SO D: 16 GB.	
Servidor Web Canales	Node	Windows Server 2019 Standard o Datacenter x64. Nombre físico. IP LAN. IP Pública. Windows Server 2019 Standard or Datacenter x64. RAM 8 GB. CPU 64 Bits. 4 Cores de 2 Ghz. Discos SO C: 126 GB. SO D: 16 GB.	

Nombre	Tipo	Documentación	Propiedad
Trabajo de despliegue lappiz.com	Technology Process		
Trabajo de despliegue: yaml	Technology Process		
Trabajo de integración lappiz.com	Technology Process		
Trabajo de integración: yaml	Technology Process		
cc:PGN SUI (módulo central)	Application Collaboration	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN.	
cc:Presentación	Application Collaboration	Submódulo de presentación del SUI. interfaz gráfica, interfaz web visible a los usuarios clientes y funcionarios de la PGN.	

Organización. 1n. Mapa producto

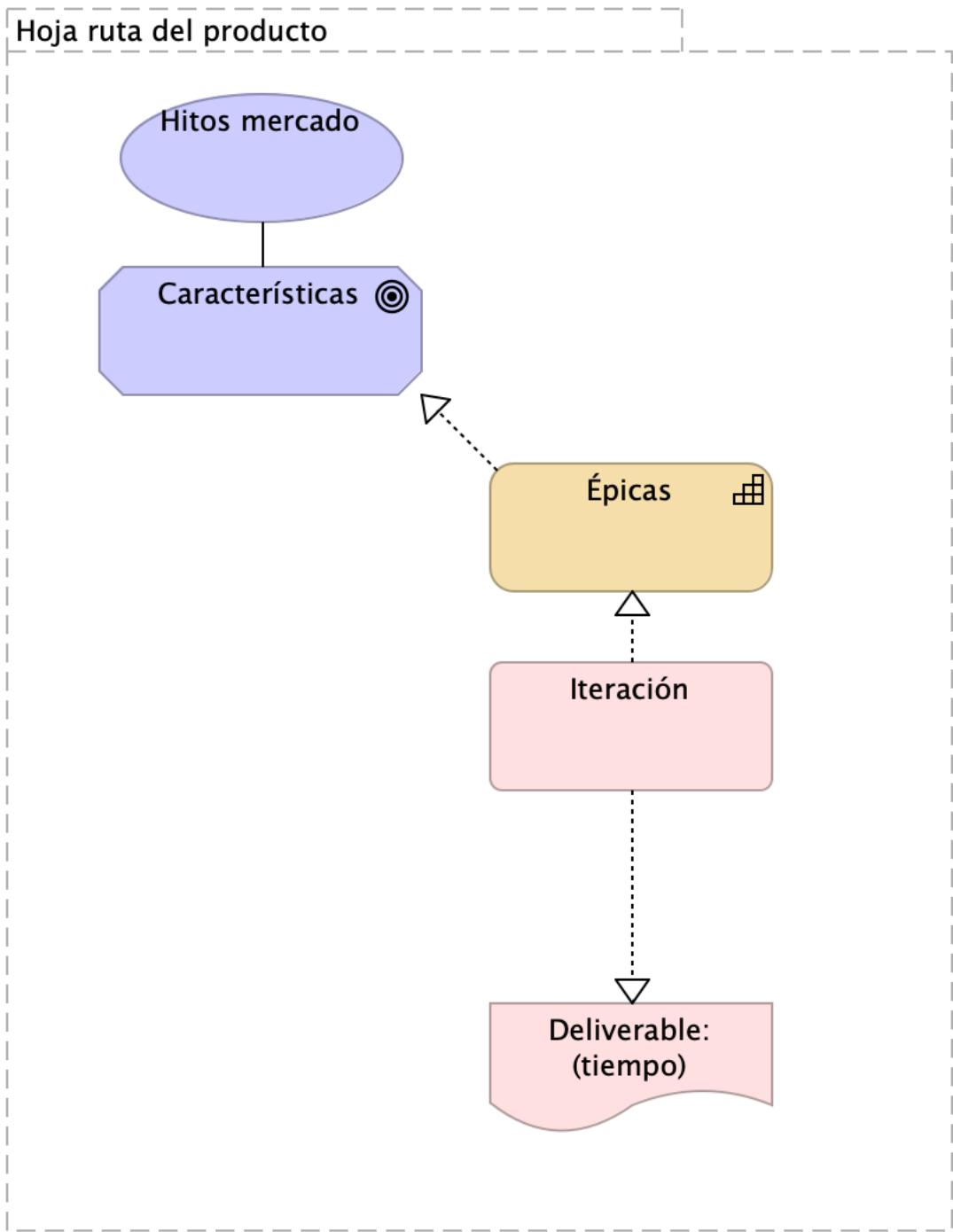


Imagen 40: Organización. 1n. Mapa producto

Fuente: *Repositorio arquitectura Mi Mutual (2023)*

Catálogo de Elementos

Tabla 37: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
Características	Goal		

Nombre	Tipo	Documentación	Propiedad
Deliverable: (tiempo)	Deliverable		
Hitos mercado	Value		
Hoja ruta del producto	Grouping		
Iteración	Work Package		
Tiempo	Gap		
Épicas	Capability		

Organización. 1n.1.. Mapa producto arquitectura PGN

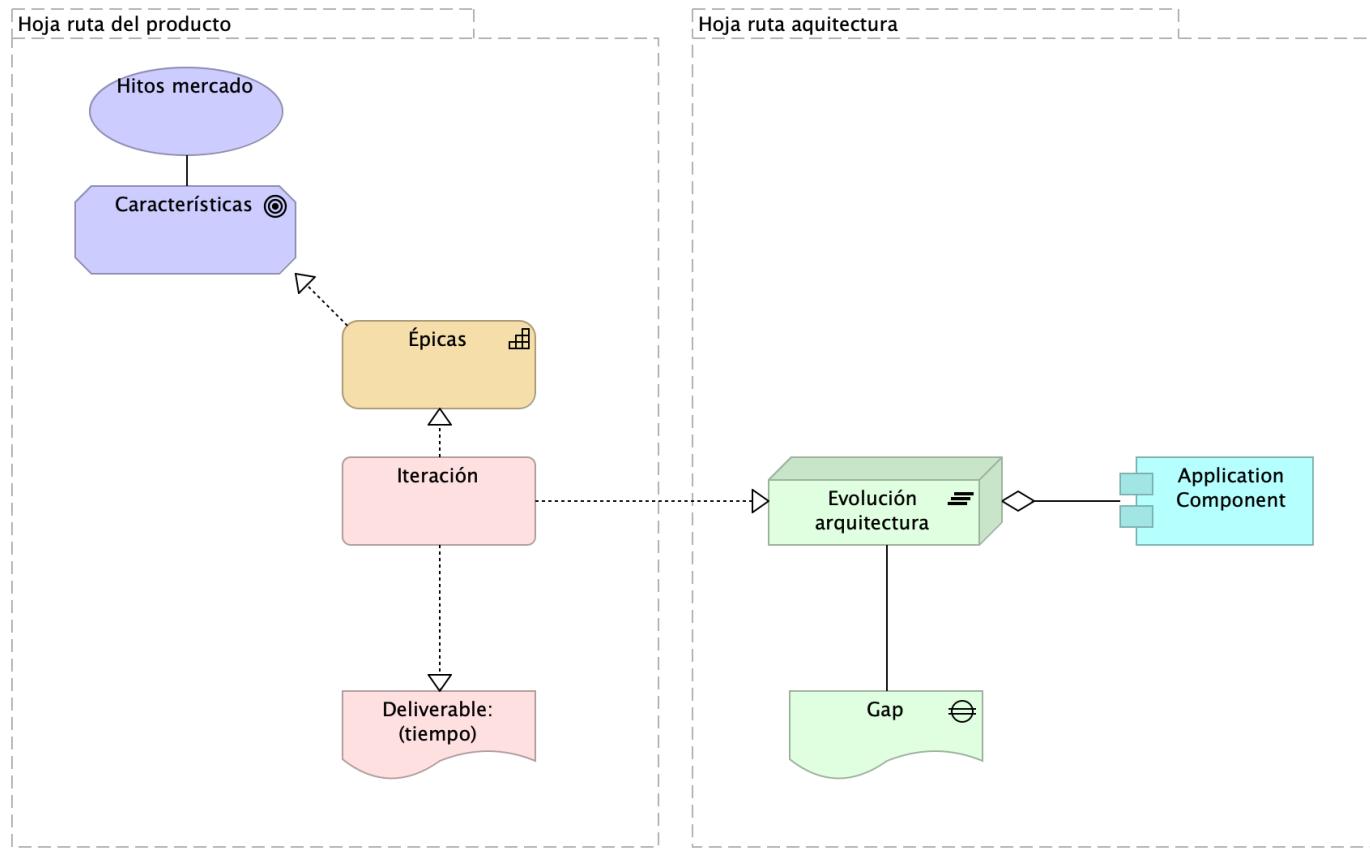


Imagen 41: Organización. 1n.1.. Mapa producto arquitectura PGN

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 38: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
Application Component	Application Component		
Características	Goal		
Deliverable: (tiempo)	Deliverable		
Evolución arquitectura	Plateau		
Gap	Gap		
Hitos mercado	Value		
Hoja ruta aquitectura	Grouping		
Hoja ruta del producto	Grouping		
Iteración	Work Package		
Épicas	Capability		

Organización. 1n.1.a. Mapa producto PGN.1.Relatoría

SIREL (Relatoría). Organización de trabajo. Características funcionales, sistémicas, seguridad.

versión 0.12

Organización y distribución de las características técnicas y funcionales del módulo de Relatoría.

Características principales: * Utilización de metadatos * Búsqueda de contenido (intradocumental y por metadatos) * Procesos de recolección y sincronización de contenidos

De arriba a abajo: 1. Fila 1, planificación de espacios de trabajo (iteraciones, para este caso) restringido al alcance del proyecto Migración PGN 2023. 1. Debajo, lo hitos importantes organizados en el tiempo. 1. Fila 3. Evolución de las características en los aspectos funcionales, técnico, hardware y software del módulo Relatoría de PGN. 1. Finalmente, fila final del diagrama, la entrega en el tiempo de las capacidades del módulo de relatoría (épicas, para el caso de Scrum). La prioridad de liberación de estas la determina el equipo funcional de este módulo de la PGN.

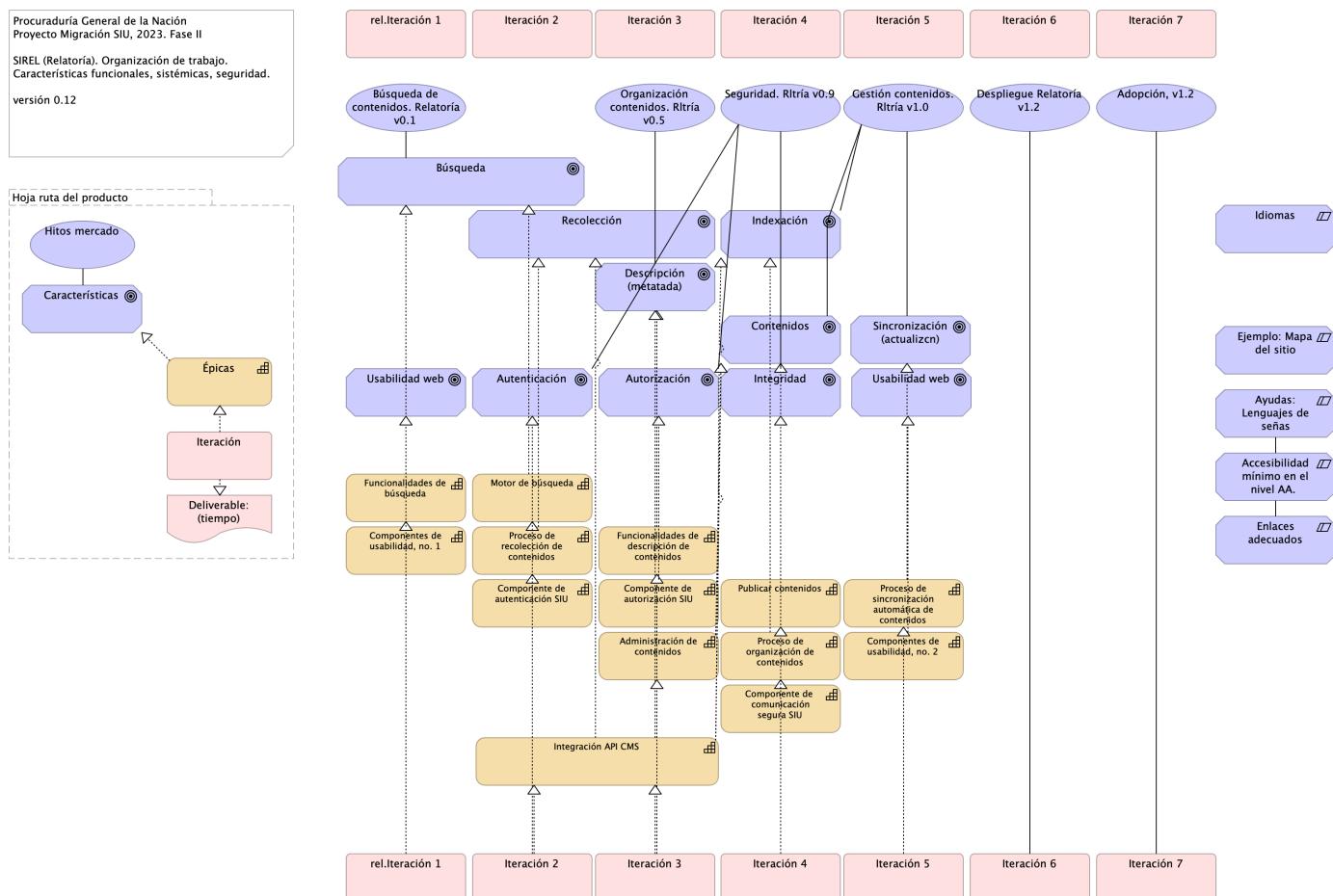


Imagen 42: Organización. 1n.1.a. Mapa producto PGN.1.Relatoría

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Nombre	Tipo	Documentación	Propiedad
Accesibilidad mínima en el nivel AA.	Constraint	Características:	

- Inclusión para los contenidos auditivos, subtítulos incorporados o textos escondidos, (Closed Caption).

- Inclusión de lengua de señas Colombiana para interacciones con la ciudadanía.

||| Administración de contenidos | Capability ||| Adopción, v1.2 | Value ||| Autenticación | Goal ||| Autorización | Goal ||| Ayudas: Lenguajes de señas | Constraint ||| Búsqueda | Goal ||| Búsqueda de contenidos. Relatoría v0.1 | Value ||| Características | Goal ||| Componente de comunicación segura SIU | Capability ||| Componente de autenticación SIU | Capability ||| Componente de autorización SIU | Capability ||| Componentes de usabilidad, no. 1 | Capability ||| Componentes de usabilidad, no. 2 | Capability ||| Contenidos | Goal | Se tendrán que adecuar los contenidos auditivos de los sitios web, con subtítulos o Closed Caption y la apropiación de lenguajes de señas. ||| Deliverable: (tiempo) | Deliverable ||| Descripción (metatada) | Goal ||| Despliegue Relatoría v1.2 | Value ||| Ejemplo: Mapa del sitio | Constraint | Capa que permita reforzar las busquedas en los motores de Busquedas, y que ayude a facilitar la accesibilidad de los usuarios, de forma

que pueda estar indexada de forma adecuada.

Características:

Mayor Navegación del sitio.

Mejor referenciación de contenido.

Mayor facilidad de búsqueda en los Mavegadores web.

| | | Enlaces adecuados | Constraint | Los enlaces deberan ser identificados de forma clara, y el indicativo del sitio o la ventana que se abrirá o la ruta al documento que llegará.

| | | Funcionalidades de búsqueda | Capability | | | Funcionalidades de descripción de contenidos | Capability | | | Gestión contenidos. Rlría v1.0 | Value | | | Hitos mercado | Value | | | Hoja ruta del producto | Grouping | | | Idiomas | Constraint | Tener en cuenta el idioma del sitio web, para que en el marco del contexto de ubicación pueda ser interpretado, de acuerdo con el país de ubicación. | | | Indexación | Goal | | | Integración API CMS | Capability | | | Integridad | Goal | | | Iteración | Work Package | | | Iteración 2 | Work Package | | | Iteración 3 | Work Package | | | Iteración 4 | Work Package | | | Iteración 5 | Work Package | | | Iteración 6 | Work Package | | | Iteración 7 | Work Package | | | Motor de búsqueda | Capability | | | Organización contenidos. Rlría v0.5 | Value | | | Proceso de organización de contenidos | Capability | | | Proceso de recolección de contenidos | Capability | | | Proceso de sincronización automática de contenidos | Capability | | | Publicar contenidos | Capability | | | Recolección | Goal | | | Seguridad. Rlría v0.9 | Value | | | Sincronización (actualizcn) | Goal | | | Usabilidad web | Goal | | | rel.Iteración 1 | Work Package | | | Épicas | Capability | | |

Table: Elementos de la vista. {#tbl:tblelement-Organización.1n.1.a.MapaproductoPGN.1.Relatoría-id}

Organización. 1n.1.b. Mapa producto PGN. Relatoría

Procuraduría General de la Nación Proyecto Migración SIU, 2023. Fase II

Relatoría. Organización de trabajo. Características funcionales, sistémicas, seguridad.

versión 0.7

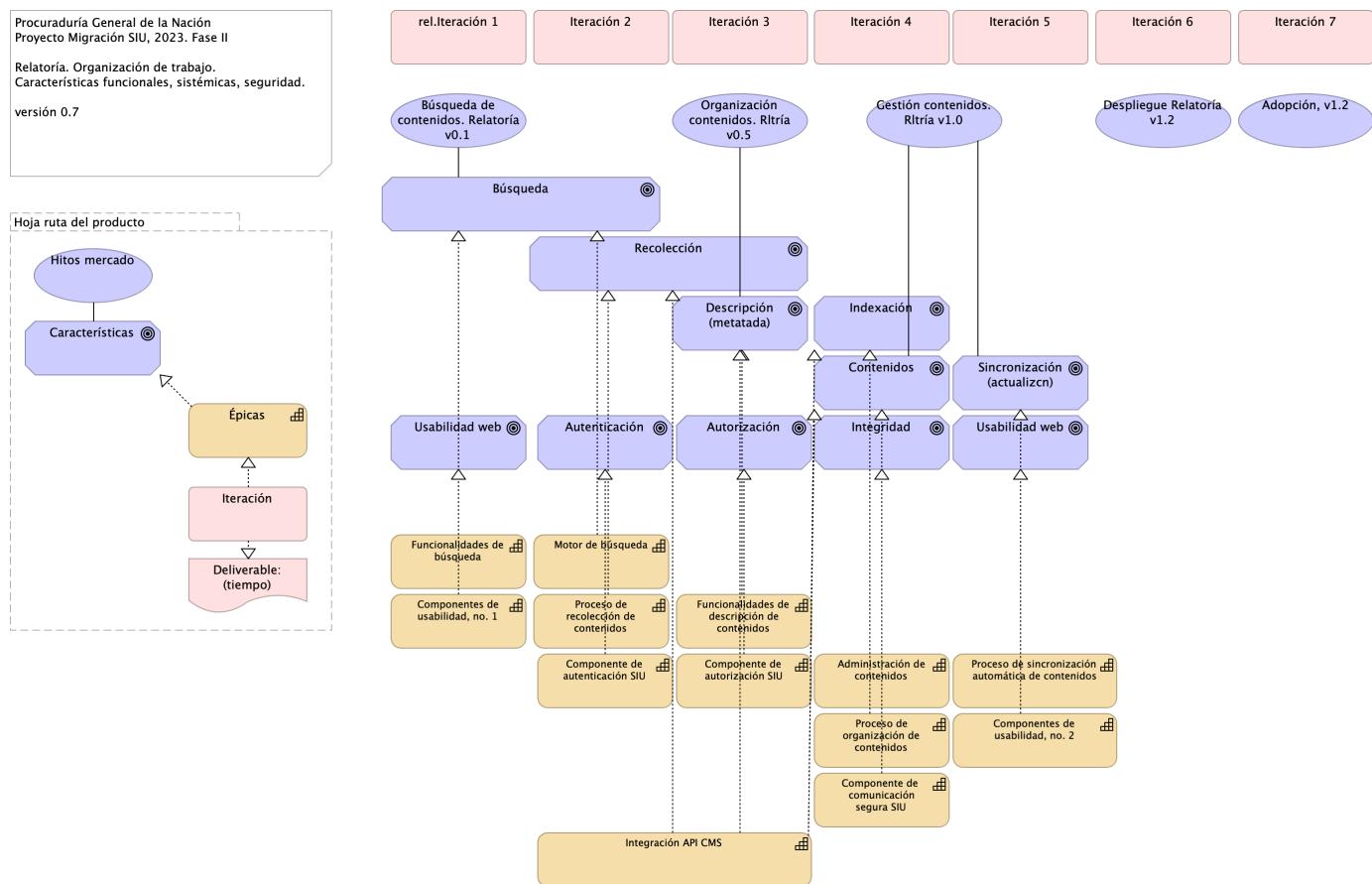


Imagen 43: Organización. 1n.1.b. Mapa producto PGN. Relatoría

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 39: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
Administración de contenidos	Capability		

Nombre	Tipo	Documentación	Propiedad
Adopción, v1.2	Value		
Autenticación	Goal		
Autorización	Goal		
Búsqueda	Goal		
Búsqueda de contenidos. Relatoría v0.1	Value		
Características	Goal		
Componente de comunicación segura SIU	Capability		
Componente de autenticación SIU	Capability		
Componente de autorización SIU	Capability		
Componentes de usabilidad, no. 1	Capability		
Componentes de usabilidad, no. 2	Capability		
Contenidos	Goal	Se tendrán que adecuar los contenidos audiovisuales de los sitios web, con subtítulos o Closed Caption y la apropiación de lenguajes de señas.	
Deliverable: (tiempo)	Deliverable		
Descripción (metatada)	Goal		
Despliegue Relatoría v1.2	Value		
Funcionalidades de búsqueda	Capability		
Funcionalidades de descripción de contenidos	Capability		
Gestión contenidos. Rltría v1.0	Value		
Hitos mercado	Value		
Hoja ruta del producto	Grouping		
Indexación	Goal		
Integración API CMS	Capability		
Integridad	Goal		
Iteración	Work Package		
Iteración 2	Work Package		
Iteración 3	Work Package		
Iteración 4	Work Package		
Iteración 5	Work Package		
Iteración 6	Work Package		
Iteración 7	Work Package		
Motor de búsqueda	Capability		
Organización contenidos. Rltría v0.5	Value		
Proceso de organización de contenidos	Capability		
Proceso de recolección de contenidos	Capability		
Proceso de sincronización automática de contenidos	Capability		
Recolección	Goal		
Sincronización (actualizcn)	Goal		
Usabilidad web	Goal		
rel.Iteración 1	Work Package		
Épicas	Capability		

Organización. 2n.1. Mapa producto PGN. Conciliacion

Procuraduría General de la Nación Proyecto Migración SIU, 2023. Fase II

Conciliación Administrativa (...). Organización de trabajo. Características funcionales, sistémicas, seguridad.

versión 0.1

Procuraduría General de la Nación
Proyecto Migración SIU, 2023, Fase II
Conciliación Administrativa (...). Organización de trabajo.
Características funcionales, sistémicas, seguridad.
versión 0.1

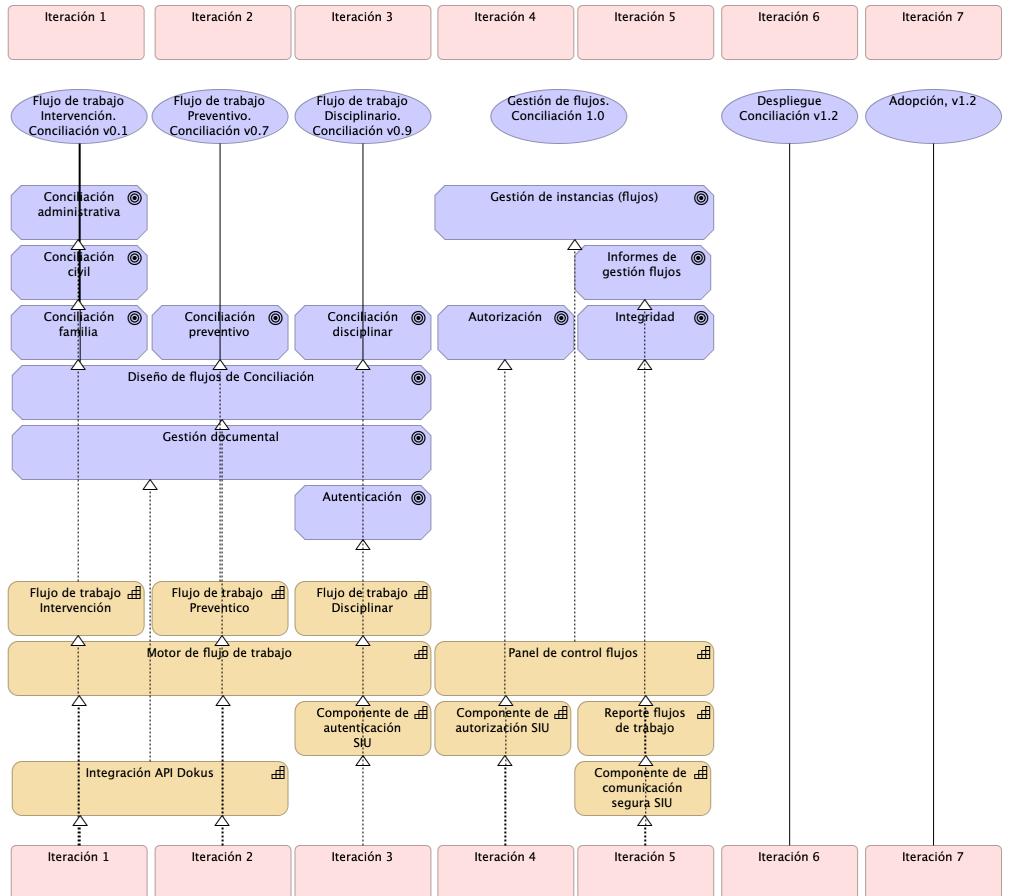
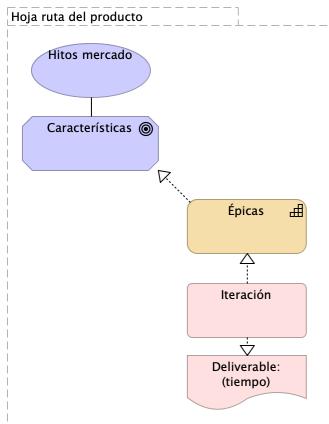


Imagen 44: Organización. 2n.1. Mapa producto PGN. Conciliacion

Fuente: *Repositorio arquitectura Mi Mutual (2023)*

Catálogo de Elementos

Tabla 40: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
Adopción, v1.2	Value		
Autenticación	Goal		
Autorización	Goal		
Características	Goal		
Componente de comunicación segura SIU	Capability		
Componente de autenticación SIU	Capability		
Componente de autorización SIU	Capability		
Conciliación administrativa	Goal		
Conciliación civil	Goal		
Conciliación disciplinaria	Goal		
Conciliación familia	Goal		
Conciliación preventivo	Goal		
Deliverable: (tiempo)	Deliverable		
Despliegue Conciliación v1.2	Value		
Diseño de flujos de Conciliación	Goal		
Flujo de trabajo Preventico	Capability		
Flujo de trabajo Disciplinar	Capability		
Flujo de trabajo Disciplinario. Conciliación v0.9	Value		
Flujo de trabajo Intervención	Capability		
Flujo de trabajo Intervención. Conciliación v0.1 (copy)	Value		
Flujo de trabajo Preventivo. Conciliación v0.7	Value		
Gestión de flujos. Conciliación 1.0	Value		
Gestión de instancias (flujos)	Goal		

Nombre	Tipo	Documentación	Propiedad
Gestión documental	Goal		
Hitos mercado	Value		
Hoja ruta del producto	Grouping		
Informes de gestión flujos	Goal		
Integración API Dokus	Capability		
Integridad	Goal		
Iteración	Work Package		
Iteración 1	Work Package		
Iteración 2	Work Package		
Iteración 3	Work Package		
Iteración 4	Work Package		
Iteración 5	Work Package		
Iteración 6	Work Package		
Iteración 7	Work Package		
Motor de flujo de trabajo	Capability		
Panel de control flujos	Capability		
Reporte flujos de trabajo	Capability		
Épicas	Capability		

Organización. 2n.1a. Mapa producto PGN. Conciliacion

Procuraduría General de la Nación Proyecto Migración SIU, 2023. Fase II

Conciliación. Intervención, Preventivo y Disciplinario. Organización de trabajo. Características funcionales, sistémicas, seguridad.

versión 0.3

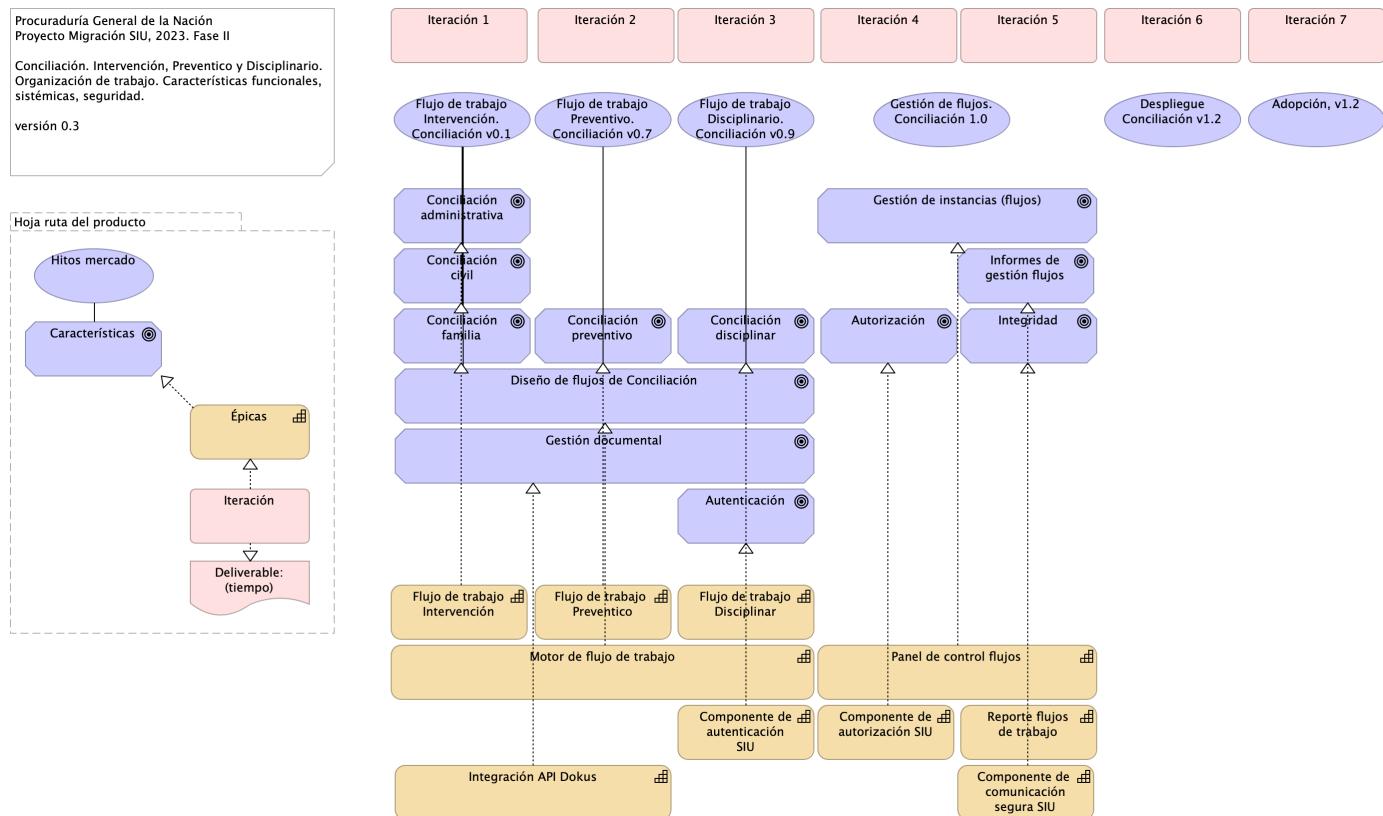


Imagen 45: Organización. 2n.1a. Mapa producto PGN. Conciliacion

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 41: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
Adopción, v1.2	Value		
Autenticación	Goal		
Autorización	Goal		
Características	Goal		
Componente de comunicación segura SIU	Capability		
Componente de autenticación SIU	Capability		
Componente de autorización SIU	Capability		
Conciliación administrativa	Goal		
Conciliación civil	Goal		
Conciliación disciplinar	Goal		
Conciliación familia	Goal		
Conciliación preventivo	Goal		
Deliverable: (tiempo)	Deliverable		
Despliegue Conciliación v1.2	Value		
Diseño de flujos de Conciliación	Goal		
Flujo de trabajo Preventico	Capability		
Flujo de trabajo Disciplinar	Capability		
Flujo de trabajo Disciplinario. Conciliación v0.9	Value		
Flujo de trabajo Intervención	Capability		
Flujo de trabajo Intervención. Conciliación v0.1 (copy)	Value		
Flujo de trabajo Preventivo. Conciliación v0.7	Value		
Gestión de flujos. Conciliación 1.0	Value		
Gestión de instancias (flujos)	Goal		
Gestión documental	Goal		
Hitos mercado	Value		
Hoja ruta del producto	Grouping		
Informes de gestión flujos	Goal		
Integración API Dokus	Capability		
Integridad	Goal		
Iteración	Work Package		
Iteración 1	Work Package		
Iteración 2	Work Package		
Iteración 3	Work Package		
Iteración 4	Work Package		
Iteración 5	Work Package		
Iteración 6	Work Package		
Iteración 7	Work Package		
Motor de flujo de trabajo	Capability		
Panel de control flujos	Capability		
Reporte flujos de trabajo	Capability		
Épicas	Capability		

Organización. 3n.1. Mapa producto PGN. SIAF

Procuraduría General de la Nación Proyecto Migración SIU, 2023. Fase II

SIAF. Inventario PGN. Organización de trabajo. Características funcionales, sistémicas, seguridad.

versión 0.2

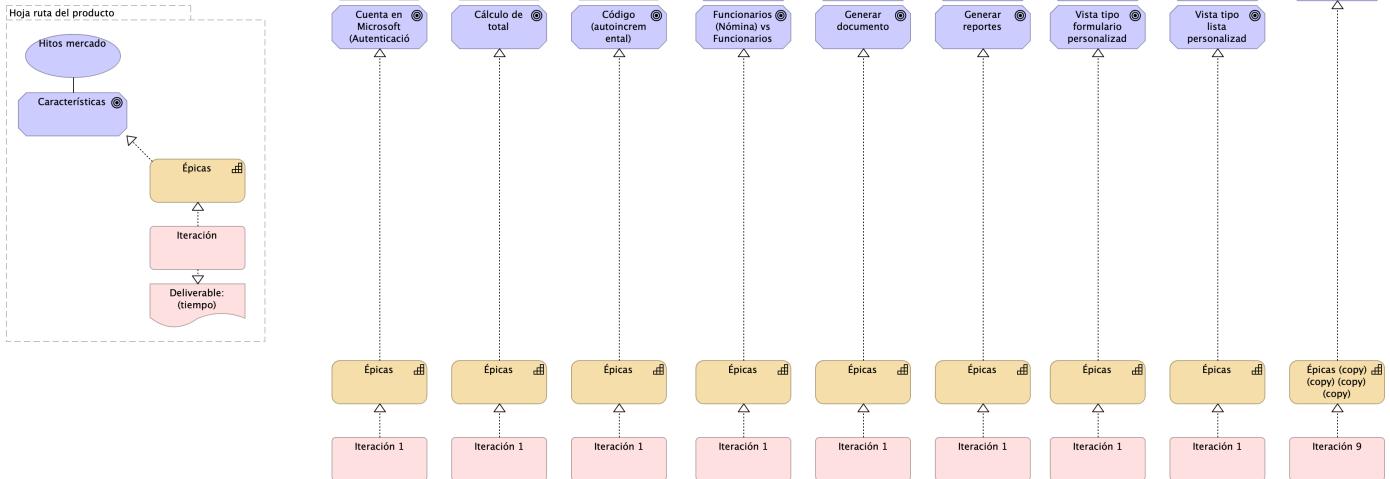


Imagen 46: Organización. 3n.1. Mapa producto PGN. SIAF

Fuente: *Repository arquitectura Mi Mutual (2023)*

Catálogo de Elementos

Tabla 42: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
Acciones de acuerdo al estado	Goal	Realización de acciones específicas según el estado de los movimientos devolutivos.	
Almacén	Goal	Administración de almacenes.	
Asientos	Goal	Registro de asientos.	
CRUD Campos	Goal	Operaciones CRUD (Crear, Leer, Actualizar, Eliminar) en campos de los asientos.	
Características	Goal		
Creación de movimiento	Goal	Generación de movimientos de acuerdo con los asientos abiertos.	
Cuenta de funcionario	Goal	Gestión de cuentas de funcionarios.	
Cuenta en Microsoft (Autenticación)	Goal	Autenticación mediante cuentas de Microsoft.	
Cálculo de total	Goal	Cálculo automático del total basado en la información de elementos.	
Código (autoincremental)	Goal	Generación automática de códigos que se reinician cada año.	
Deliverable: (tiempo)	Deliverable		
Dependiendo del tipo de movimiento	Goal	Gestión de movimientos según su tipo, incluyendo elementos como conceptos, beneficiarios y funcionarios (maestros).	
Elementos	Goal	Registro de elementos relacionados con los movimientos.	
Estado	Goal	Seguimiento del estado de los asientos.	
Fecha automática	Goal	Asignación automática de la fecha en los asientos.	
Filtrar por campos	Goal	Capacidad para filtrar los movimientos devolutivos según campos específicos.	

Nombre	Tipo	Documentación	Propiedad
Funcionario Posesionado	Goal	Registro de información sobre funcionarios en posesión.	
Funcionarios (Nómina) vs Funcionarios (Siaf)	Goal	Comparación y actualización de información de funcionarios almacenada en Siaf con la información de nómina.	
Generar documento	Goal	Creación de documentos relacionados con los movimientos.	
Generar reportes	Goal	Creación de informes y reportes para proporcionar la información solicitada.	
Hitos mercado	Value		
Hoja ruta del producto	Grouping		
Iteración	Work Package		
Iteración 1	Work Package		
Iteración 1	Work Package		
Iteración 1	Work Package		
Iteración 1	Work Package		
Iteración 1	Work Package		
Iteración 1	Work Package		
Iteración 1	Work Package		
Iteración 1	Work Package		
Iteración 1	Work Package		
Iteración 9	Work Package		
Login (Doble factor)	Goal	Autenticación de usuario mediante doble factor de seguridad	
Movimiento Consumible	Goal	Registro de movimientos relacionados con elementos consumibles.	
Movimiento devolutivo	Goal	Registro de movimientos devolutivos.	
Sincronización con Homminis	Goal	Sincronización de datos con el sistema Homminis.	
Vista CRUD	Goal	Interfaz para crear, leer, actualizar y eliminar registros en el almacén.	
Vista formulario personalizada	Goal	Personalización de formularios para la creación de asientos dependiendo del almacén.	
Vista tipo formulario personalizada	Goal	Personalización de formularios para ingresar datos relacionados con los asientos.	
Vista tipo lista personalizada	Goal	Visualización personalizada en forma de lista con filtros por campos específicos.	
Épicas	Capability		
Épicas (copy) (copy) (copy) (copy)	Capability		

Organización. 4n.1. Mapa producto PGN. Estratego

Procuraduría General de la Nación Proyecto Migración SIU, 2023. Fase II

Conciliación. Intervención, Preventico y Estratego. Reportes estratégicos PGN. Organización de trabajo. Características funcionales, sistémicas, seguridad.

versión 0.2

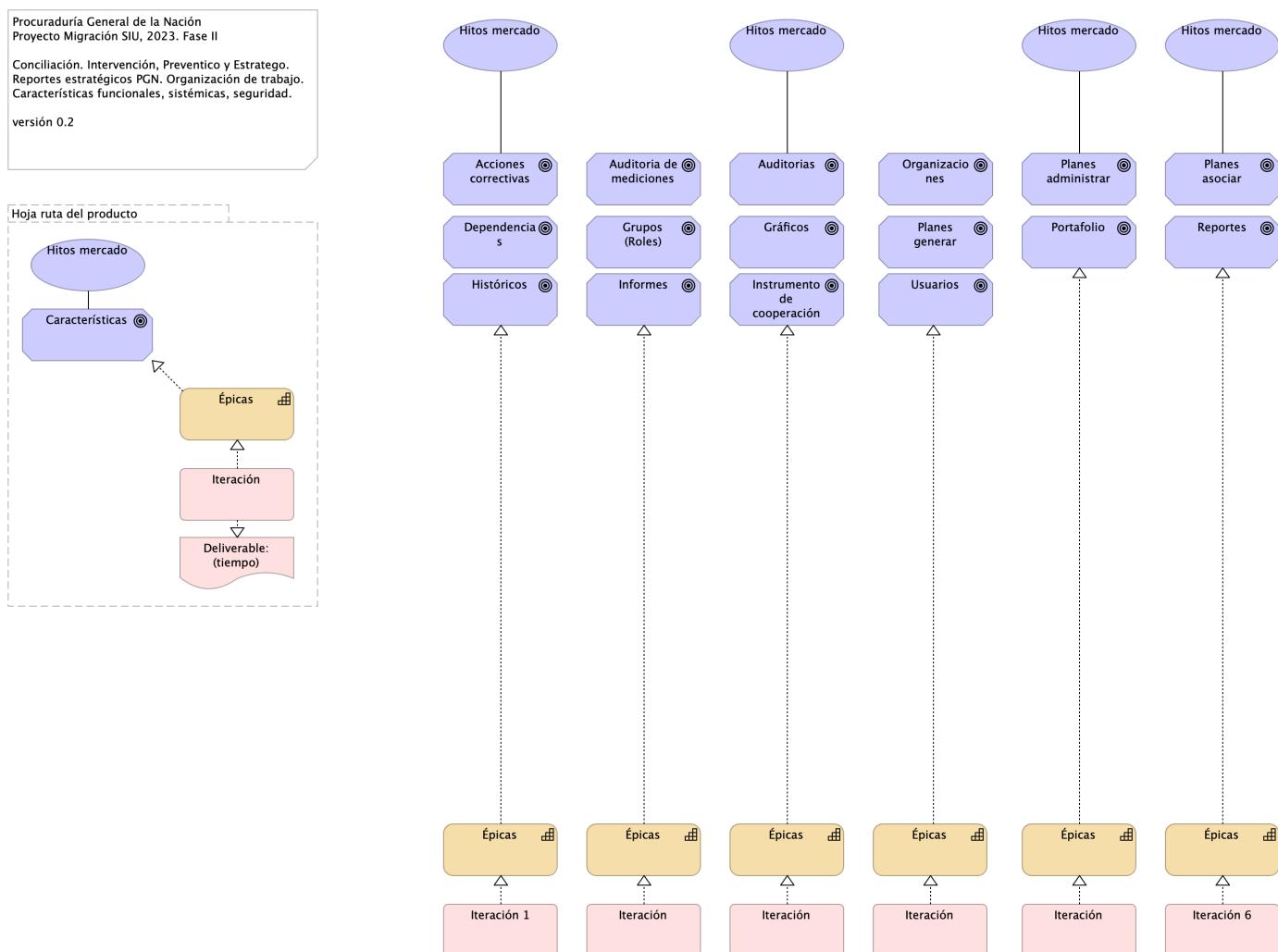


Imagen 47: Organización. 4n.1. Mapa producto PGN. Estratego

Fuente: *Repositorio arquitectura Mi Mutual (2023)*

Catálogo de Elementos

Tabla 43: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
Acciones correctivas	Goal	Administrar los riesgos asociados a cada uno de los indicadores o planes.	
Auditoria de mediciones	Goal	Gestionar las actividades de los usuarios, como el registro de indicadores, el tipo, etc.	
Auditorias	Goal	Gestionar el control de logs de las actividades realizadas por el usuario en sesión.	
Características	Goal		
Deliverable: (tiempo)	Deliverable		
Dependencias	Goal	Reportar al sistema, actividades, proyectos, indicadores.	
Grupos (Roles)	Goal	Administrar los roles y permisos dentro del sistema	

Nombre	Tipo	Documentación	Propiedad
Gráficos	Goal	Generar y presentar gráficos	
Históricos	Goal	Almacenar y consultar históricos dentro del sistema	
Hitos mercado	Value		
Hoja ruta del producto	Grouping		
Informes	Goal	Generar documentos con los informes correspondientes.	
Instrumento de cooperación	Goal	Administrar los proyectos de los cooperantes.	
Iteración	Work Package		
Iteración 1	Work Package		
Iteración 6	Work Package		
Organizaciones	Goal	Estructura principal.	
Planes administrar	Goal	Administrar el plan estratégico institucional.	
Planes asociar	Goal	Asociar recursos, presupuesto.	
Planes generar	Goal	Generar planes estratégicos institucionales y asociar los planes de acción preventivos.	
Portafolio	Goal	Gestionar el portafolio de todos los proyectos de la entidad.	
Reportes	Goal	Generar reportes y exportarlos en diferentes tipos de archivo.	
Usuarios	Goal	Administrar los usuarios del sistema	
Épicas	Capability		

Organización. 4n.1a. Mapa producto PGN. Comparativa

Procuraduría General de la Nación Proyecto Migración SIU, 2023. Fase II

Mapa de Producto SIAF, Estratego. Comparativa funcional, técnica y de impacto.

versión 0.2

Mapa de productos. Comparativa funcional y técnica de módulos PGN, SIAF (izq.) y Estratego (derecha).

Volumen Funcional

El análisis funcional de ambos módulos realizado durante el levantamiento (iteración 0) del presente proyecto arroja que SIAF tiene un 40% más de volumen que Estratego. Esto es, 16 funcionalidades de Estratego, mientras que SIAF suma 26. Ver imagen comparativa.

Viabilidad de Alcance

Tomando en cuenta el criterio de calidad de la migración, objeto del presente contrato, 078-2023, de migrar módulos completos dentro de lo posible, y contrastando este criterio con el plazo del proyecto actual, que es de 4 meses, de los cuales ya se han ejecutado aproximadamente el 20% del mismo, es

más viable la estrategia de migración de Estratego sobre la de SIAF de la PGN por requerir menos iteraciones de desarrollo: seis (6) iteraciones, versus, nueve (9) de SIAF.

Impacto / Beneficio a PGN

Los hitos de mercado del presente análisis producto, imagen arriba, dan cuenta del beneficio e impacto de ambos proyectos de migración. Haciendo la comparación de los hitos de mercado de estos productos resalta que Estratego prima sobre SIAF en tanto que el peso cualitativo de las funciones estratégicas del primero son de mayor relevancia que las funciones operativas de inventario de SIAF. Basado en esto, Estratego reporta mayor beneficio y menos impacto en esfuerzo (por la razón anterior) que SIAF.

En conclusión, por los criterios de viabilidad y tamaño funcional y por el impacto estratégico, Estratego resulta en la migración a seleccionar sobre la del modulo SIAF. Esta estrategia satisface además la restricción de migrar moóulos completos sobre migración parcial.

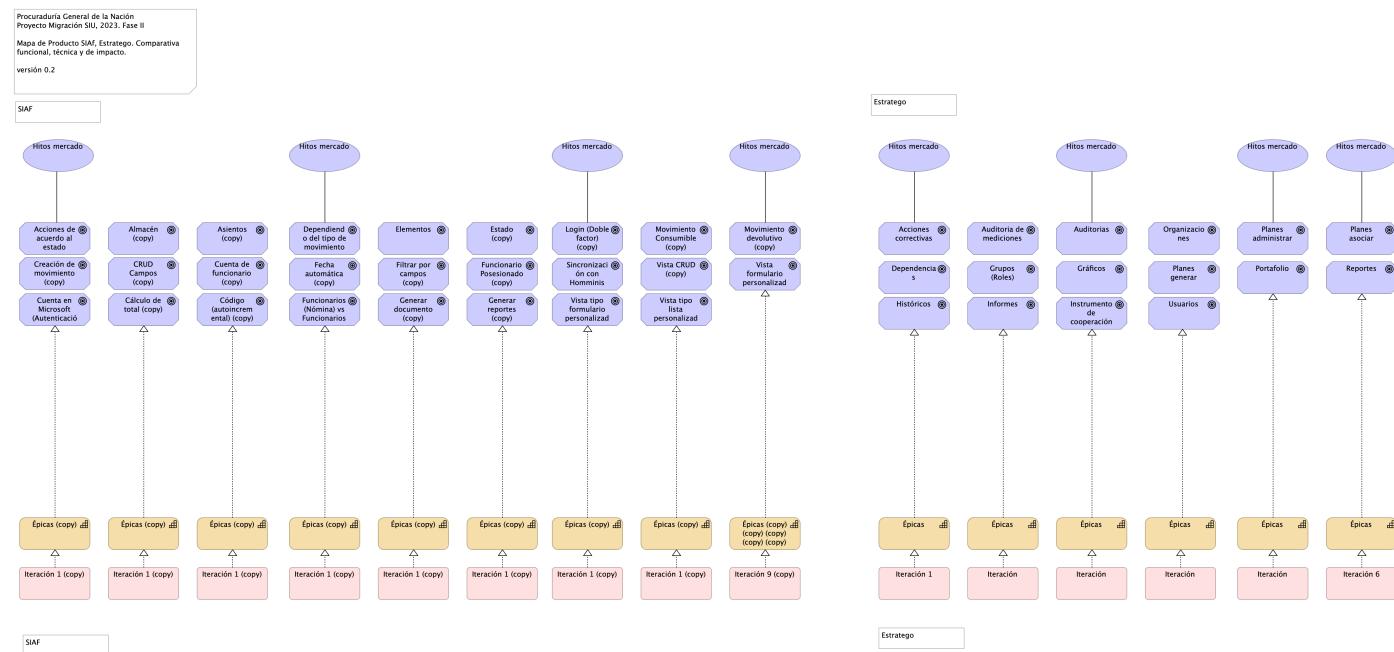


Imagen 48: Organización. 4n.1a. Mapa producto PGN. Comparativa

Fuente: *Repository arquitectura Mi Mutual (2023)*

Catálogo de Elementos

Tabla 44: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
Acciones correctivas	Goal	Administrar los riesgos asociados a cada uno de los indicadores o planes.	
Acciones de acuerdo al estado (copy)	Goal	Realización de acciones específicas según el estado de los movimientos devolutivos.	
Almacén (copy)	Goal	Administración de almacenes.	
Asientos (copy)	Goal	Registro de asientos.	
Auditoria de mediciones	Goal	Gestionar las actividades de los usuarios, como el registro de indicadores, el tipo, etc.	
Auditorias	Goal	Gestionar el control de logs de las actividades realizadas por el usuario en sesión.	
CRUD Campos (copy)	Goal	Operaciones CRUD (Crear, Leer, Actualizar, Eliminar) en campos de los asientos.	
Creación de movimiento (copy)	Goal	Generación de movimientos de acuerdo con los asientos abiertos.	
Cuenta de funcionario (copy)	Goal	Gestión de cuentas de funcionarios.	
Cuenta en Microsoft (Autenticación) (copy)	Goal	Autenticación mediante cuentas de Microsoft.	

Nombre	Tipo	Documentación	Propiedad
Iteración 6	Work Package		
Iteración 9 (copy)	Work Package		
Login (Doble factor) (copy)	Goal	Autenticación de usuario mediante doble factor de seguridad	
Movimiento Consumible (copy)	Goal	Registro de movimientos relacionados con elementos consumibles.	
Movimiento devolutivo (copy)	Goal	Registro de movimientos devolutivos.	
Organizaciones	Goal	Estructura principal.	
Planes administrar	Goal	Administrar el plan estratégico institucional.	
Planes asociar	Goal	Asociar recursos, presupuesto.	
Planes generar	Goal	Generar planes estratégicos institucionales y asociar los planes de acción preventivos.	
Portafolio	Goal	Gestionar el portafolio de todos los proyectos de la entidad.	
Reportes	Goal	Generar reportes y exportarlos en diferentes tipos de archivo.	
Sincronización con Homminis (copy)	Goal	Sincronización de datos con el sistema Homminis.	
Usuarios	Goal	Administrar los usuarios del sistema	
Vista CRUD (copy)	Goal	Interfaz para crear, leer, actualizar y eliminar registros en el almacén.	
Vista formulario personalizada (copy)	Goal	Personalización de formularios para la creación de asientos dependiendo del almacén.	
Vista tipo formulario personalizada (copy)	Goal	Personalización de formularios para ingresar datos relacionados con los asientos.	
Vista tipo lista personalizada (copy)	Goal	Visualización personalizada en forma de lista con filtros por campos específicos.	
Épicas	Capability		
Épicas (copy)	Capability		
Épicas (copy) (copy) (copy) (copy) (copy)	Capability		

Riesgos.1. Migración funcional

Riesgos de la migración funcional:

- RSG1. Estrategia CMS central
- RSG2. Motor de búsqueda
- RSG3. Estatego como BI
- RSG4. Conciliación y Doku

- RSG5. Gestión de sesiones / caducidad
- RSG6. Componentes de negocio
- RSG7. Asignación de roles y permisos de Acceso
- RSG8. Intentos de accesos no autorizados
- RSG9. Alteración de datos negocio
- RSG10. Validación decisiones de arquitectura

Acciones de Mitigación

1. Informar a la PGN de las implicaciones junto con alternativas para la implementación de la acción de aprovechamiento: diseño del SCM central (sharepoint). La PGN debe decidir si o no a la acción propuesta.
2. Informar a la PGN de las implicaciones junto con alternativas para la implementación de la acción de aprovechamiento: diseño del motor de búsqueda compartido (sharepoint). La PGN debe decidir si o no a la acción propuesta.
3. Informar a la PGN de las implicaciones junto con alternativas para la implementación de la acción de manejo del riesgo: diseño de solución de inteligencia de negocio (Power BI). La PGN debe decidir si o no a la acción propuesta.
4. Informar a la PGN de las implicaciones junto con alternativas para la implementación de la acción de manejo del riesgo: ubicar la lógica, los flujos, y los datos misionales dentro del SIU. La PGN debe decidir si o no a la acción propuesta.
5. Informar a la PGN de las implicaciones junto con alternativas para la implementación de la acción de manejo del riesgo: facilitar la administración de seguridad en un solo lugar (distinto de localizarla en las aplicaciones web). La PGN debe decidir si o no a la acción propuesta.

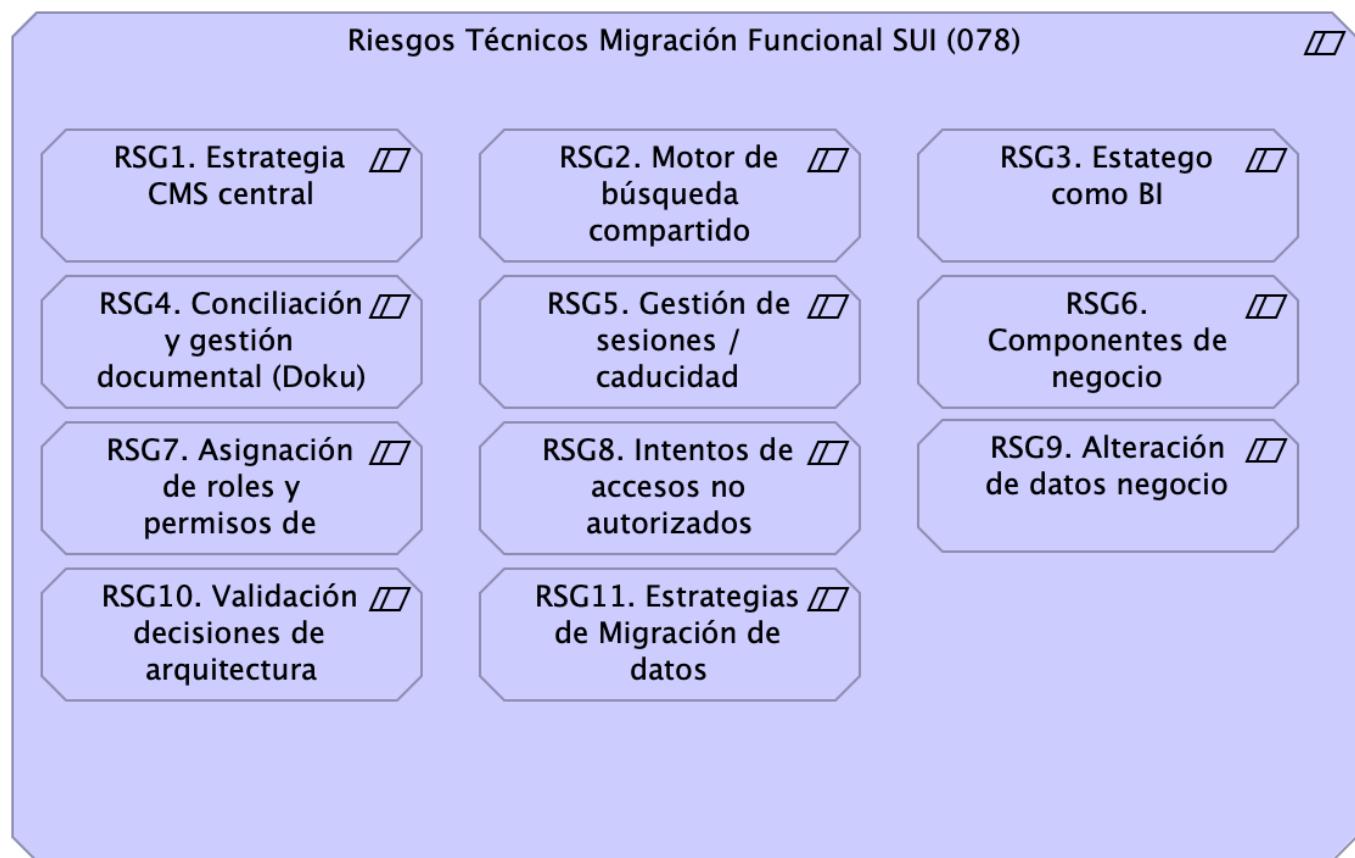


Imagen 49: Riesgos.1. Migración funcional

Fuente: *Repositorio arquitectura Mi Mutual (2023)*

Catálogo de Elementos

Nombre	Tipo	Documentación	Propiedad
RSG1. Estrategia CMS central	Constraint	Establecer desde el principio el gestor de contenidos compartido que los módulos del SUI migrados van a usar.	

Nombre	Tipo	Documentación	Propiedad
RSG10. Validación decisiones de arquitectura	Constraint	Discutir la arquitectura de referencia de SUI Migración PGN. La arquitectura de referencia SUI informa de todas las fortalezas y consideraciones estructurales y de sistema, como extensibilidad, rendimiento y seguridad, que regirán a todos los módulos del SUI migrado.	
RSG11. Estrategias de Migración de datos	Constraint	Discutir el alcance y los recursos para la correcta migración de datos incluidos en contrato 078, Migración Funcional SIU en atención al numeral 5.6 del anexo técnico del proyecto.	5.6 MIGRACIÓN DE DATOS
RSG2. Motor de búsqueda compartido	Constraint	Establecer desde el principio el motor de búsqueda de conteidos compartido para los módulos del SUI migrados.	
RSG3. Estatego como BI	Constraint	Definir la arquitectura de Estatego migrado: puede ser una solución de BI simple, o puede ser una aplicación web tradicional.	
RSG4. Conciliación y gestión documental (Doku)	Constraint	Definir la ubicación de los componentes misionales de Conciliación Administrativa (SIU). Debe estar fuera de Doku.	
RSG5. Gestión de sesiones / caducidad	Constraint	Establecer desde el principio el motor de búsqueda de conteidos compartido para los módulos del SUI migrados.	
RSG6. Componentes de negocio	Constraint	Incluir el esfuerzo de creación de componentes estructurales y comunes a los módulos del SUI migrado requeridos por la arquitectura de referencia SUI. Algunos componentes requeridos son: * Administración de autorizaciones (integrado con el directorio PGN) * Motor de flujos de trabajo para diseño y organización del trabajo (Conciliación) * Componente de ruteo de documentos (Relatoría)	
RSG7. Asignación de roles y permisos de Acceso	Constraint	RSG7. Asignación de roles y permisos de Acceso	

Los riesgos de autenticación como el Single Sign On (SSO), permite que si las credenciales de usuario se ven comprometidas, pueden dar permiso a un atacante acceder a todos o la mayoría de recursos y aplicaciones en la red.

Se ha propuesto controlar los accesos a partir de la documentación que identifica la metodología de clasificación y gestión de usuarios roles y procesos de autenticación, a partir del control de acceso basado en roles RBAC (Identidades y autenticación), que permite tener una reacción más oportuna para controlar los accesos a diferentes módulos de los diferentes sistemas de Información. Los inicios de sesión de los usuarios asociados a cuenta de dominio de Active Directory deben tener en cuenta la asignación de roles de ingreso al servidor o roles de ingreso al motor de bases de datos. Las cuentas de usuario no deben ser creadas de administrador local (administrador), es una puerta de entrada para los ataques de fuerza bruta.

| | | RSG8. Intentos de accesos no autorizados | Constraint | RSG8. Intentos de accesos no autorizados

Los intentos no autorizados son una de las técnicas más comunes utilizadas en la actualidad, los diferentes tipos de amenazas de intrusiones SQL Injections, Denegaciones de Servicios, riesgos de Ransomware, Ingeniería social, malware y otras amenazas, permite que se proponga implementación de soluciones de Seguridad perimetral a partir de la implementación de WAF para controlar las peticiones externas y evaluación de vulnerabilidades y escaneo para conocer puertos abiertos y establecer medidas.

| | | RSG9. Alteración de datos negocio | Constraint | RSG9. Alteración de datos almacenados en Base de Datos.

Se deberán asignar usuarios para la conexión de cada base de datos.

Se debe proporcionar seguridad a nivel de filas y columnas (ofuscamiento) para proteger los datos confidenciales en el nivel de columnas y filas RLS ((seguridad de nivel de fila)).

Algunos de los métodos y características que se deben tener en cuenta a implementar es a partir del Alway encrypted, para cifrar los datos que se

encuentran almacenados.

| | | Riesgos Técnicos Migración Funcional SUI (078) | Constraint | Conjunto de riesgos técnicos y arquitectura. Proyecto Migración SUI 2023, PGN.

| |

Table: Elementos de la vista. {#tbl:tblelement-Riesgos.1.Migraciónfuncional-id}

Riesgos.2. Modelo Riesgo RSG10

Procuraduría General de la Nación Proyecto Migración SIU, 2023. Fase II

Gestión de riesgos técnicos. RSG10. Validación decisiones de arquitectura. Agentes del riesgo, valoración, plan de acción.

versión 0.5

Para mitigar el riesgo 10, RSG10. Validación decisiones de arquitectura, que tiene como agente de riesgo a los arquitectos del contratista, Softgic, y al de la entidad, PGN, es necesario iniciar un proceso de evaluación y aprobación de la arquitectura. La frecuencia de este proceso será eventual, y como mínimo una vez cada dos semanas.

Valoración del Riesgo

Tabla 45: Valoración del riesgo RSG10. Validación decisiones de arquitectura. Migración SUI.

Requisito	Extensibilidad SUI
Descripción	Concentración de los componentes de negocio, misionales, del SUI protegidos de cambios provenientes de otros sistemas. Ver Patrón de Diseño Migración SUI, más adelante en el documento.
Calidad sistémica	La extensibilidad que optimiza el diseño Migración SUI está dada por el intercambio de submódulos no misionales, como el gestor documental, sin afectación de los componentes misionales que este diseño protege.

Procuraduría General de la Nación
Proyecto Migración SIU, 2023. Fase II

Gestión de riesgos técnicos. RSG10. Validación decisiones de arquitectura. Agentes del riesgo, valoración, plan de acción.

versión 0.5

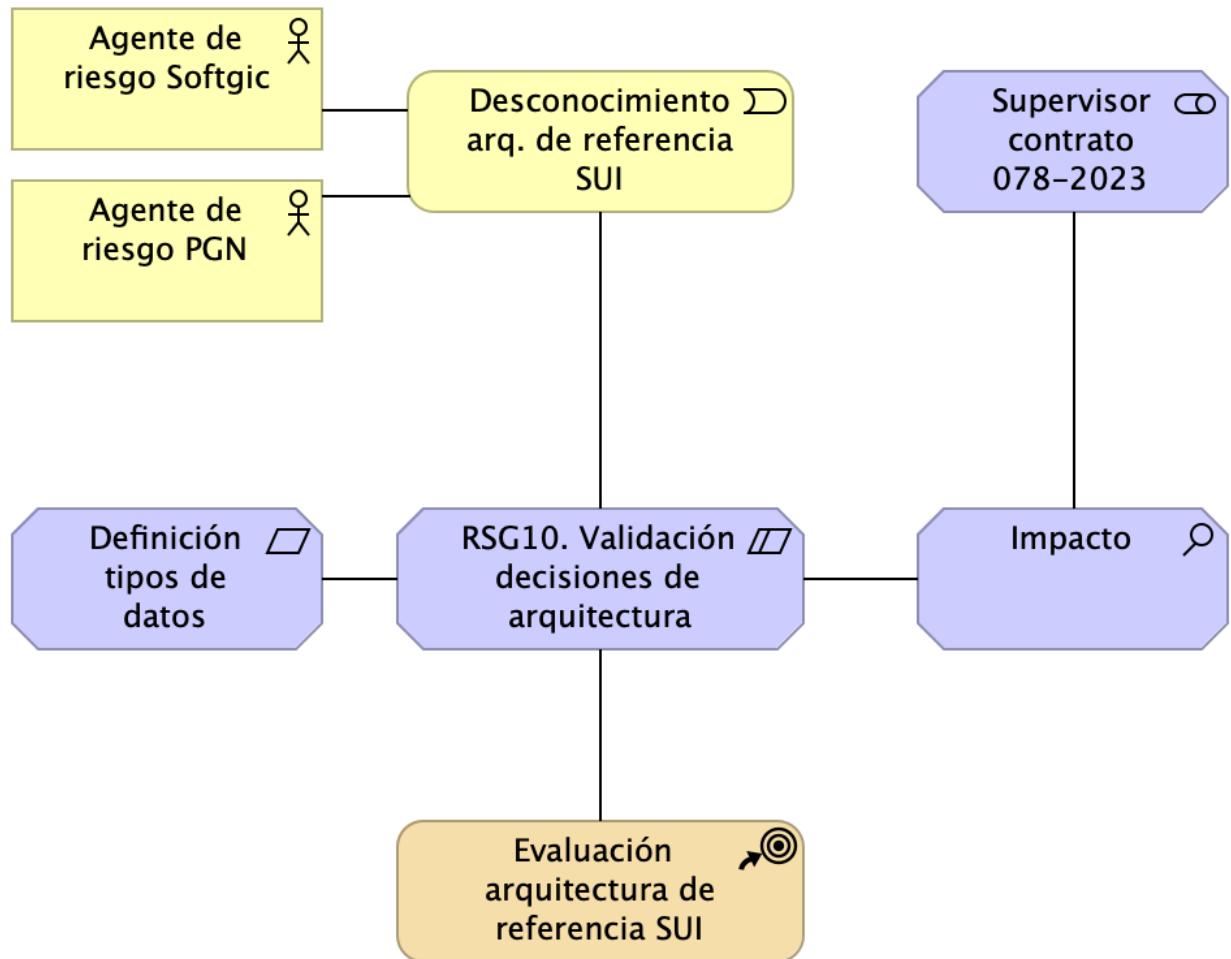


Imagen 50: Riesgos.2. Modelo Riesgo RSG10

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 46: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
Agente de riesgo PGN	Business Actor	Arquitecto PGN	
Agente de riesgo Softgic	Business Actor	Arquitecto Softgic	
Definición tipos de datos módulos SUI	Requirement		
Desconocimiento arq. de referencia SUI	Business Event		
Evaluación arquitectura de referencia SUI	Course Of-Action	La frecuencia del proceso de evaluación de la arquitectura es eventual, mínimo una vez cada dos semanas.	
Impacto	Assessment		

Nombre	Tipo	Documentación	Propiedad
RSG10. Validación decisiones de arquitectura	Constraint	Discutir la arquitectura de referencia de SUI Migración PGN. La arquitectura de referencia SUI informa de todas las fortalezas y consideraciones estructurales y de sistema, como extensibilidad, rendimiento y seguridad, que regirán a todos los módulos del SUI migrado.	
Supervisor contrato 078-2023	Stakeholder		

Riesgos.3. Modelo Riesgo RSG11

Procuraduría General de la Nación Proyecto Migración SIU, 2023. Fase II

Gestión de riesgos técnicos. RSG11. Estrategias de migración de datos módulos migrados. Agentes del riesgo, valoración, plan de acción.

versión 0.5

Para mitigar el riesgo 10, RSG10. Validación decisiones de arquitectura, que tiene como agente de riesgo a los arquitectos del contratista, Softgic, y al de la entidad, PGN, es necesario iniciar un proceso de evaluación y aprobación de la arquitectura. La frecuencia de este proceso será eventual, y como mínimo una vez cada dos semanas.

Valoración del Riesgo

Tabla 47: Valoración del riesgo RSG10. Validación decisiones de arquitectura. Migración SUI.

Requisito	Extensibilidad SUI
Descripción	Concentración de los componentes de negocio, misionales, del SUI protegidos de cambios provenientes de otros sistemas. Ver Patrón de Diseño Migración SUI, más adelante en el documento.
Calidad sistémica	La extensibilidad que optimiza el diseño Migración SUI está dada por el intercambio de submódulos no misionales, como el gestor documental, sin afectación de los componentes misionales que este diseño protege.

Gestión de riesgos técnicos. RSG11. Estrategias de migración de datos módulos migrados.
Agentes del riesgo, valoración, plan de acción.

versión 0.5

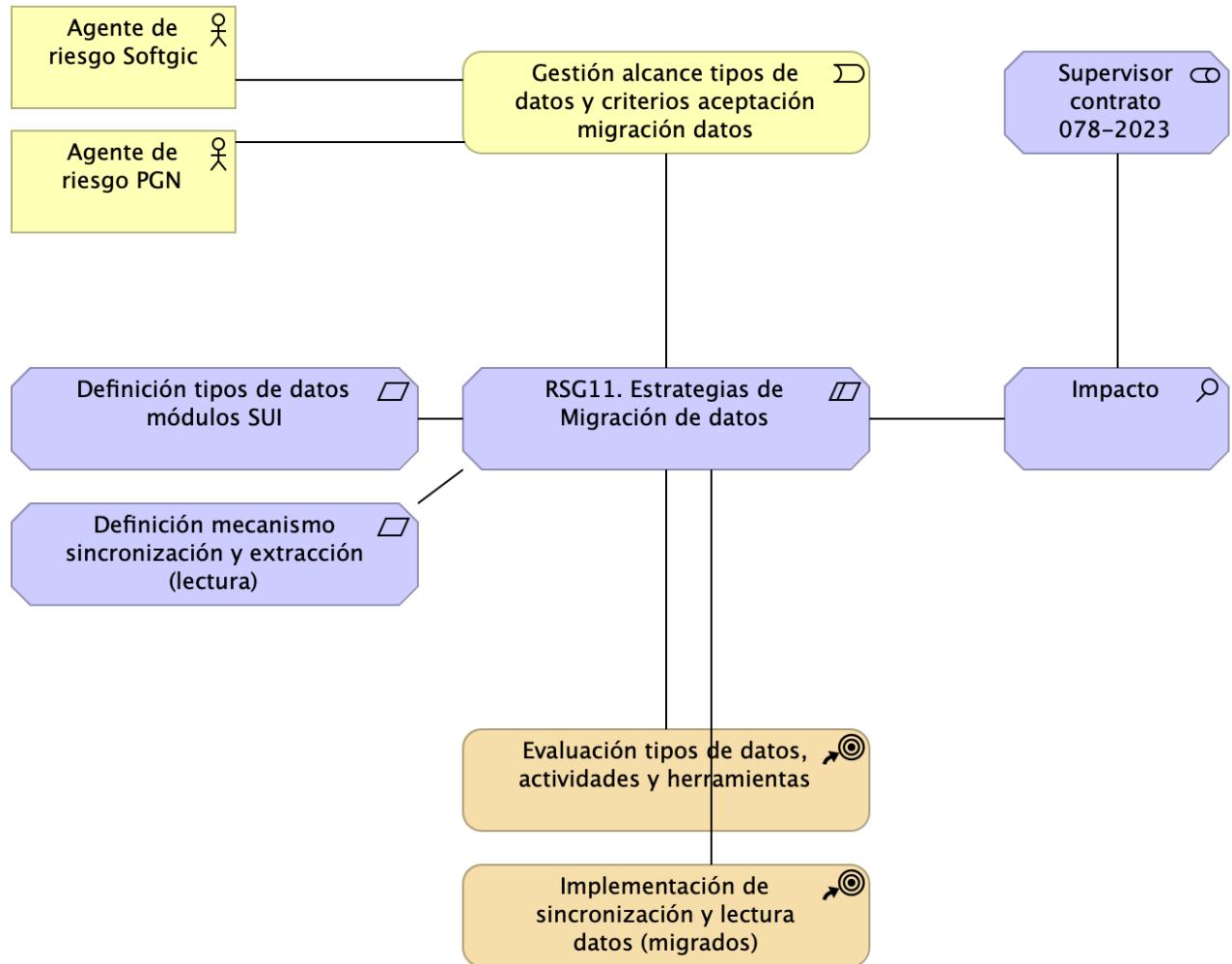


Imagen 51: Riesgos.3. Modelo Riesgo RSG11

Fuente: *Repositorio arquitectura Mi Mutual (2023)*

Catálogo de Elementos

Tabla 48: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
Agente de riesgo PGN	Business Actor	Arquitecto PGN	
Agente de riesgo Softgic	Business Actor	Arquitecto Softgic	
Definición mecanismo sincronización y extracción (lectura)	Requirement		
Definición tipos de datos módulos SUI	Requirement		
Evaluación tipos de datos, actividades y herramientas	Course Of-Action	La frecuencia del proceso de evaluación de la arquitectura es eventual, mínimo una vez cada dos semanas.	
Gestión alcance tipos de datos y criterios aceptación migración datos	Business Event		
Impacto	Assessment	Sobretrabajo del proyecto 078, esfuerzo y presupuesto.	

Nombre	Tipo	Documentación	Propiedad
Implementación de sincronización y lectura datos (migrados)	Course Of-Action	La frecuencia del proceso de evaluación de la arquitectura es eventual, mínimo una vez cada dos semanas.	
RSG11. Estrategias de Migración de datos	Constraint	Discutir el alcance y los recursos para la correcta migración de datos incluidas en contrato 078, Migración Funcional SIU en atención al numeral 5.6 del anexo técnico del proyecto.	5.6 MIGRACIÓN DE DATOS
Supervisor contrato 078-2023	Stakeholder		

Seguridad Migracion.1a.SIU submódulos

PGN. Migración Sistemas Misionales. Fase 2.

Submódulos Sistema Único de Información. Requerimientos asociados a submódulos.

versión 0.3

Identificación de submódulos del Sistema Único de Información (SUI) de la PGN.

Todos los sistemas de información del SUI siguen esta directiva: estarán constituidos por submódulos dispuestos en relación de utilitarios (que sirven) a los componentes misionales del SUI, ubicados en el centro en la diagrama.

Los submódulos del SUI, tal como están presentados, reúnen a las partes que tienen el mismo rol en favor de la coherencia. Así mismo, estos pueden ser intercambiados o ampliados sin perjuicio del SUI gracias a las interfaces de unión (en favor de la extensibilidad).

Las interfaces de unión indicadas arriba obligan a los submódulos a cumplir las exigencias de los componentes misionales del SUI.

Los submódulos identificados tienen los siguientes roles para el SUI migrado:

1. cc:Presentación
2. cc:Servicios de aplicación
3. cc:Portales y canales
4. cc:Administración y configuración
5. cc:Almacenamiento

Requerimientos Asociados a los Submódulos

La disposición de los módulos y submódulos presentada, denominada SUI Migración en adelante, facilita la focalización de los requerimientos encontrados en el levantamiento realizado por el actual proyecto. Así, por ejemplo, los requerimientos funcionales se encuentran concentrados en el submódulo de presentación (ver imagen).

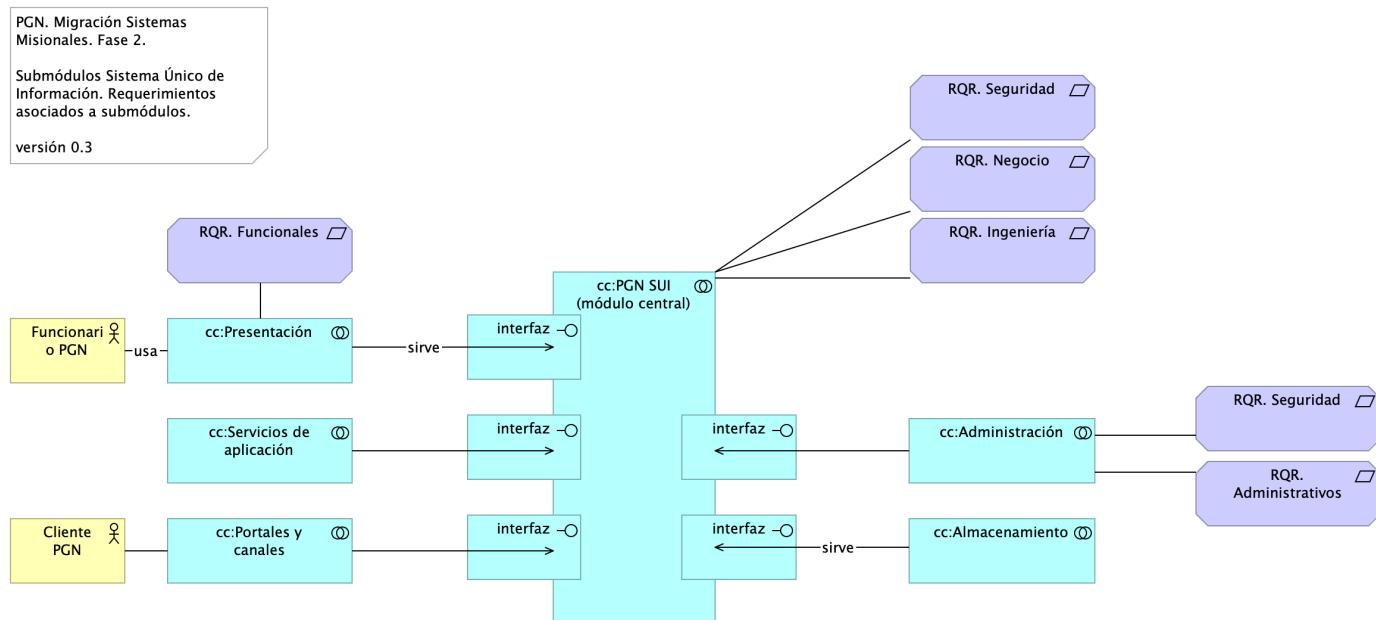


Imagen 52: Seguridad Migracion.1a.SIU submódulos

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Tabla 49: Elementos de la vista.

Nombre	Tipo	Documentación	Propiedad
Cliente PGN	Business Actor		
Funcionario PGN	Business Actor		
RQR. Administrativos	Requirement		
RQR. Funcionales	Requirement		
RQR. Ingeniería	Requirement		
RQR. Negocio	Requirement		
RQR. Seguridad	Requirement	Requerimientos de seguridad, SUI, Migración, en aspectos de comunicación, autenticación, autorización y (manejo de) sesiones.	
cc:Administración	Application Collaboration		
cc:Almacenamiento	Application Collaboration	Espacio de almacenamiento operativo y transaccional de un módulo central del SUI migrado.	
cc:PGN SUI (módulo central)	Application Collaboration	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN.	
cc:Portales y canales	Application Collaboration	Submódulo de portales internos de la PGN a donde llega el SUI. Interfaz web que usa al SUI para llegar a direcciones y subdirecciones de la PGN. La plataforma principal de portales en este contexto es Sharepoint de Microsoft.	
cc:Presentación	Application Collaboration	Submódulo de presentación del SUI. interfaz gráfica, interfaz web visible a los usuarios clientes y funcionarios de la PGN.	
cc:Servicios de aplicación	Application Collaboration	Submódulo de servicios utilitarios que sirven al SUI. Servicios variados que cumplen roles facilitadores de las actividades misionales del SUI. Ejemplos de estos servicios son los de gestión documental, implementado por Doku en el contexto de PGN.	
interfaz	Application Interface		

Seguridad. Lineabase.1a.SIU componentes (corregida)

SSL

Dependencias de infraestructura entre los servicios que integran el modelo de aplicación de SUI, Migración.

- Servidor de Canales (App PGN web y móvil)
- Servidor Web App (App SUI)
- Servidor Lappiz (Config SUI)
- Servidor BDD App (Transaccional)
- Servidor BDD Config (Configuración)

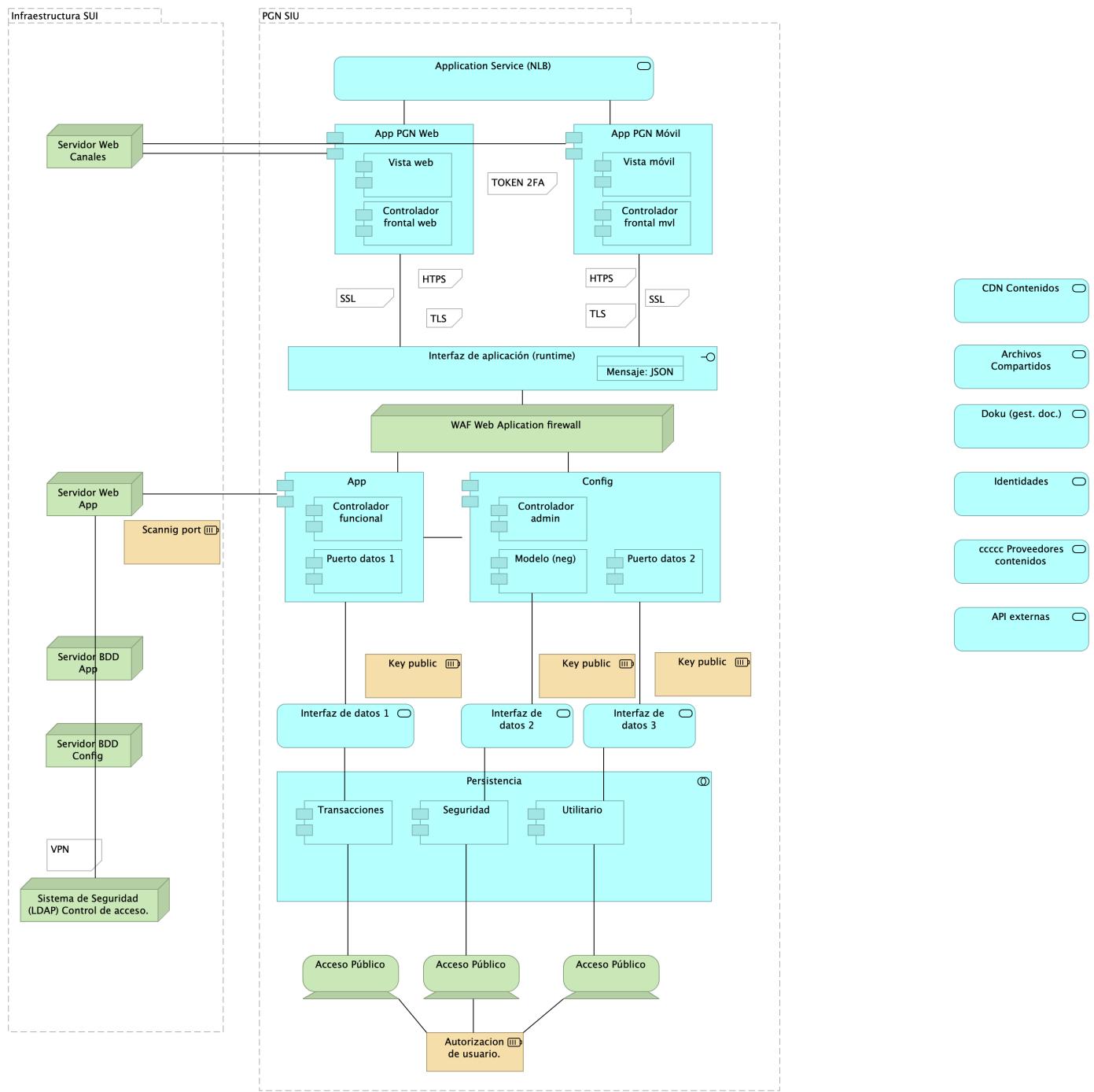


Imagen 53: Seguridad. Lineabase.1a.SIU componentes (corregida)

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Nombre	Tipo	Documentación	Propiedad
API externas	Application Service		
Acceso Público	Device		
Acceso Público	Device		
Acceso Público	Device		
App	Application Component		

Nombre	Tipo	Documentación	Propiedad
App PGN Móvil	Application Component	A partir de los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la "Guía de desarrollo OWASP" y "OWAS Cheat Sheet, se realizaran pruebas de seguridad a partir del análisis de vulnerabilidades, y pruebas de Ethical Hacking.	

Protección de datos personales,

Los sistemas de información que recogen, procesan y almacenan información de los derechos de las personas se deben almacenar de forma adecuada, la información que pueda ser vulnerada puede generar obligaciones legales y éticas con respecto a la pérdida de información confidencial por parte de ciudadanos del país.

La información contenida en las bases de datos debe tener los mecanismos de cifrado que en otros apartados se han mencionado.
La legislación que hay que tener como referencia, ley 1581 de 2012. Decreto 1377 de 2013

La metodología empleada tendrá las siguientes fases:

- FASE DE RECONOCIMIENTO:

Se recolectará toda la información posible, usando diferentes técnicas como:

- o Recopilación de dominios/IPs/puertos/servicios
- o Recopilación de metadatos
- o Uso de Google Dorks.

- ANÁLISIS DE VULNERABILIDADES:

Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.

- EXPLOTACIÓN:

Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo:

- o Inyección de código
- o Inclusión de ficheros locales o remotos
- o Evasión de autenticación
- o Carencia de controles de autorización
- o Ejecución de comandos en el lado del servidor
- o Ataques tipo Cross Site Request Forgery
- o Control de errores
- o Gestión de sesiones
- o Fugas de información
- o Secuestros de sesión
- o Comprobación de las condiciones para realizar una denegación de servicio.

- POST EXPLOTACIÓN:

En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adicionales con el objetivo de comprobar la criticidad de esta.

No URL IP

1. https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz
135.181.185.207

| | | App PGN Web | Application Component | A partir de los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la "Guía de desarrollo OWASP" y "OWAS Cheat Sheet, se realizaran pruebas de seguridad a partir del análisis de vulnerabilidades, y pruebas de Ethical Hacking.

Los resultados permitirán identificar los requisitos de seguridad que los sistemas de información o servicios web deberán cumplir.

La metodología empleada tendrá las siguientes fases:

- FASE DE RECONOCIMIENTO:

Se recolectará toda la información posible, usando diferentes técnicas como:

- o Recopilación de dominios/IPs/puertos/servicios
- o Recopilación de metadatos
- o Uso de Google Dorks.

- ANÁLISIS DE VULNERABILIDADES:

Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.

- EXPLOTACIÓN:

Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo:

- o Inyección de código
- o Inclusión de ficheros locales o remotos
- o Evasión de autenticación
- o Carencia de controles de autorización
- o Ejecución de comandos en el lado del servidor
- o Ataques tipo Cross Site Request Forgery
- o Control de errores

- o Gestión de sesiones
- o Fugas de información
- o Secuestros de sesión
- o Comprobación de las condiciones para realizar una denegación de servicio.

• POST EXPLOTACIÓN:

En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adicionales con el objetivo de comprobar la criticidad de esta.

No URL IP

1. https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz
135.181.185.207

El Login deberá evidenciar el control de errores, al momento de realizar la validación deberá mensaje de error para el caso que se autentique con credenciales erradas. | | | Application Service (NLB) | Application Service | | | Archivos Compartidos | Application Service | | | Autorización de usuario. | Resource | Los usuarios que tendrán accesos a los diferentes sistemas de información deben tener en cuenta que las credenciales de acceso son de uso personal e intransferible, por lo tanto, se deberá hacer buen uso de las contraseñas asignadas para los diferentes aplicativos de la procuraduría General de la Nación (PGN).

Identificación de Mecanismos

Identificación de roles, privilegios

Aprovisionamiento de cuentas

Establecimiento de Mecanismos de control de acceso

| | | CDN Contenidos | Application Service | | | Config | Application Component | | | Controlador admin | Application Component | | | Controlador frontal mvl | Application Component | | | Controlador frontal web | Application Component | - Verificados los SSL, se recomienda adquirir SSL seguros, con entidades certificadoras.

Si se desea continuar con SSL de Let's Encrypt, se recomienda automatizar el proceso de actualización dado que al dejar estos en modo actualización manual es probable el olvido de esta actualización (Estos certificados se deben actualizar trimestralmente y no cuentan con las características de seguridad necesarias.

| | | Controlador funcional | Application Component | | | Doku (gest. doc.) | Application Service | | | Identidades | Application Service | | | Infraestructura SUI | Grouping | Soporte de infraestructura a los componentes del SUI Migración. Servidores y ambientes de cómputo para la ejecución del software base de los componentes misionales del SUI de PGN.

| | | Interfaz de aplicación (runtime) | Application Interface | Servidor web: Microsoft-IIS/10.0

Marco de Programación: ASP.NET

Huellas digitales identificadas:

Huella digital SHA-256 "FC:79:06:7E:F5:24:20:50:F1:C0:74:F7:85:56:B9:05:B7:33:A3:2D:44:A0:48"

Huella digital SHA1 "8C:48:BD:E2:F5:18:18:C3:85:96:68:44:2E:28:A0:68:08:2F:0A:BE"

| | | Interfaz de datos 1 | Application Service | | | Interfaz de datos 2 | Application Service | | | Interfaz de datos 3 | Application Service | | | Key public | Resource | | | Key public | Resource | | | Key public | Resource | | | Mensaje: JSON | Data Object | | | Modelo (neg) | Application Component | | | PGN SIU | Grouping | El objetivo principal de la arquitectura del SUI de la migración es la centralización de los conceptos misionales: concentrar los conceptos misionales en componentes aislados; dejar por fuera de estos componentes misionales todo lo distintos a la misionalidad de la PGN.

Los objetivos secundarios de esta arquitectura SUI de la migración son flexibilidad y extensibilidad. Dichos objetivos son independientes. Es decir, estos pueden ser maximizados sin conflicto entre ellos.

| | | Persistencia | Application Collaboration | | | Puerto datos 1 | Application Component | | | Puerto datos 2 | Application Component | | | Scanning port | Resource | Se realiza verificación y comprobación de puertos y puertas traseras cerradas, por lo cual se ejecuta el protocolo telnet, que sirve verificar la entrada a los servidores por cualquier puerto que este abierto que no tenga las protecciones de seguridad adecuadas. | | | Seguridad | Application Component | | | Servidor BDD App | Node | Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz

Discos SO C: 126 GB, Backup E: 511 GB, SQL Data F: 510 GB, SQL Log G: 510 GB, TempDB G: 63.6 GB.

| | | Servidor BDD Config | Node | Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz
Discos SO C: 80 GB, Backup E: 250 GB, SQL Data F: 250 GB, SQL Log G: 250 GB, TempDB G: 30 GB.

| | | Servidor Web App | Node | Windows Server 2019 Standard o Datacenter x64. Nombre físico. IP LAN. IP Pública. Windows Server 2019 Standard or Datacenter x64. RAM 8 GB. CPU 64 Bits. 4 Cores de 2 Ghz. Discos SO C: 126 GB. SO D: 16 GB.

| | | Servidor Web Canales | Node | Windows Server 2019 Standard o Datacenter x64. Nombre físico. IP LAN. IP Pública. Windows Server 2019 Standard or Datacenter x64. RAM 8 GB. CPU 64 Bits. 4 Cores de 2 Ghz. Discos SO C: 126 GB. SO D: 16 GB.

| | | Sistema de Seguridad (LDAP) Control de acceso. | Node | Sistema de autenticación del directorio activo. | | | Transacciones | Application Component | | | Utilitario | Application Component | | | Vista móvil | Application Component | | | Vista web | Application Component | - Verificados los SSL, se recomienda adquirir SSL seguros, con entidades certificadoras.

Si se desea continuar con SSL de Let's Encrypt, se recomienda automatizar el proceso de actualización dado que al dejar estos en modo actualización manual es probable el olvido de esta actualización (Estos certificados se deben actualizar trimestralmente y no cuentan con las características de seguridad necesarias.

4. SERVICIOS IDENTIFICADOS:

Servidor web: Microsoft-IIS/10.0

Marco de Programación: ASP.NET

Huellas digitales identificadas:

Huella digital SHA-256 "FC:79:06:7E:F5:24:20:50:F1:C0:74:F7:85:56:B9:05:B7:33:A3:2D:44:A0:48"

Huella digital SHA1 "8C:48:BD:E2:F5:18:18:C3:85:96:68:44:2E:28:A0:68:08:2F:0A:BE"

| | | WAF Web Application firewall | Node | | | ccccc Proveedores contenidos | Application Service | | |

Table: Elementos de la vista. {#tbl:tblelement-Seguridad.Lineabase.1a.SIUcomponentes(corregida)-id}

Seguridad. Linebase.2.Portal

◦ P2: Servicio de administración de identidades y acceso basado en la nube de Microsoft.

El portal es el conjunto de los elementos físicos y lógicos necesarios para la implementación de la granja de servidores de SharePoint Server 2019 para el portal de la Procuraduría.

- Servidores Web Front End
- Servidores de Aplicaciones
- Servidores de SQL Server

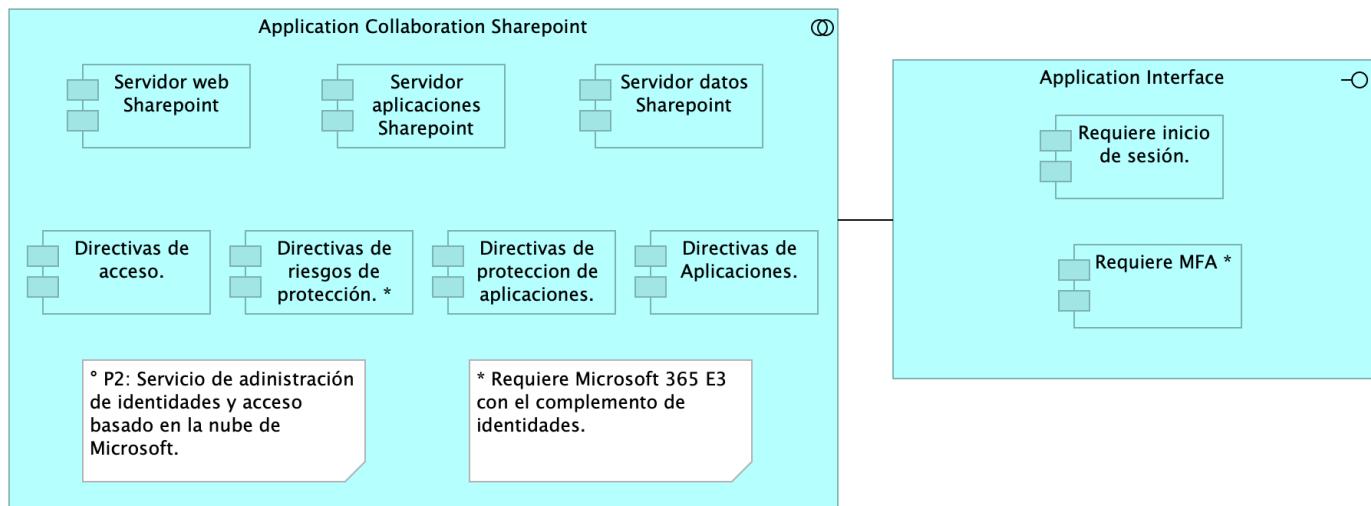


Imagen 54: Seguridad. Linebase.2.Portal

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Nombre	Tipo	Documentación	Propiedad
Application Collaboration Sharepoint	Application Collaboration		
Application Interface	Application Interface		
Directivas de Aplicaciones.	Application Component	Requiere Microsoft 365 E3 con el complemento de identidades, La restricciones de acceso a las cargas de trabajo de productividad es un elemento clave, en la que los recursos locales y en la nube se autentican y se autorizan.	
La autenticación por medio del AD con agentes que permiten ampliar su funcionalidad.			
Directivas de acceso.	Application Component	El control de acceso se da a partir de la autenticación del directorio activo, y la integración del Single Sign-On (SSO), con el inicio único de sesión fluido en todas las aplicaciones.	

Se tendrá en cuenta la implementación con multiples capas de autenticación, autenticacion multifactor MFA

| | | Directivas de proteccion de aplicaciones. | Application Component | | | Directivas de riesgos de protección. * | Application Component | | | Requiere MFA * | Application Component | Se deberá incorporar el 2FA para los accesos a la información que reposa en el SharePoint, que permita a los usuarios iniciar sesión de forma segura a través del uso de sus dispositivos móviles. | | | Requiere inicio de sesión. | Application Component | Presenta el formulario de inicio de sesión al usuario final que enviará la solicitud por medio del método POST, que envia datos de información al servidor. para que el servidor los agregue a su base de datos. | | | Servidor aplicaciones Sharepoint | Application Component | | | Servidor datos Sharepoint | Application Component | | | Servidor web Sharepoint | Application Component | | |

Table: Elementos de la vista. {#tbl:tblelement-Seguridad.Linebase.2.Portal-id}

Seguridad. Migracion.1.SIU modulos

Distribución de los servicios y paquetes que integran la aplicación de SUI.

Cuantro paquetes con tecnologías respectivas 1. Angular 11 (Web) 1. API Transaccional (Node Js) 1. API Config (C#) 1. Persistencia (SQL)

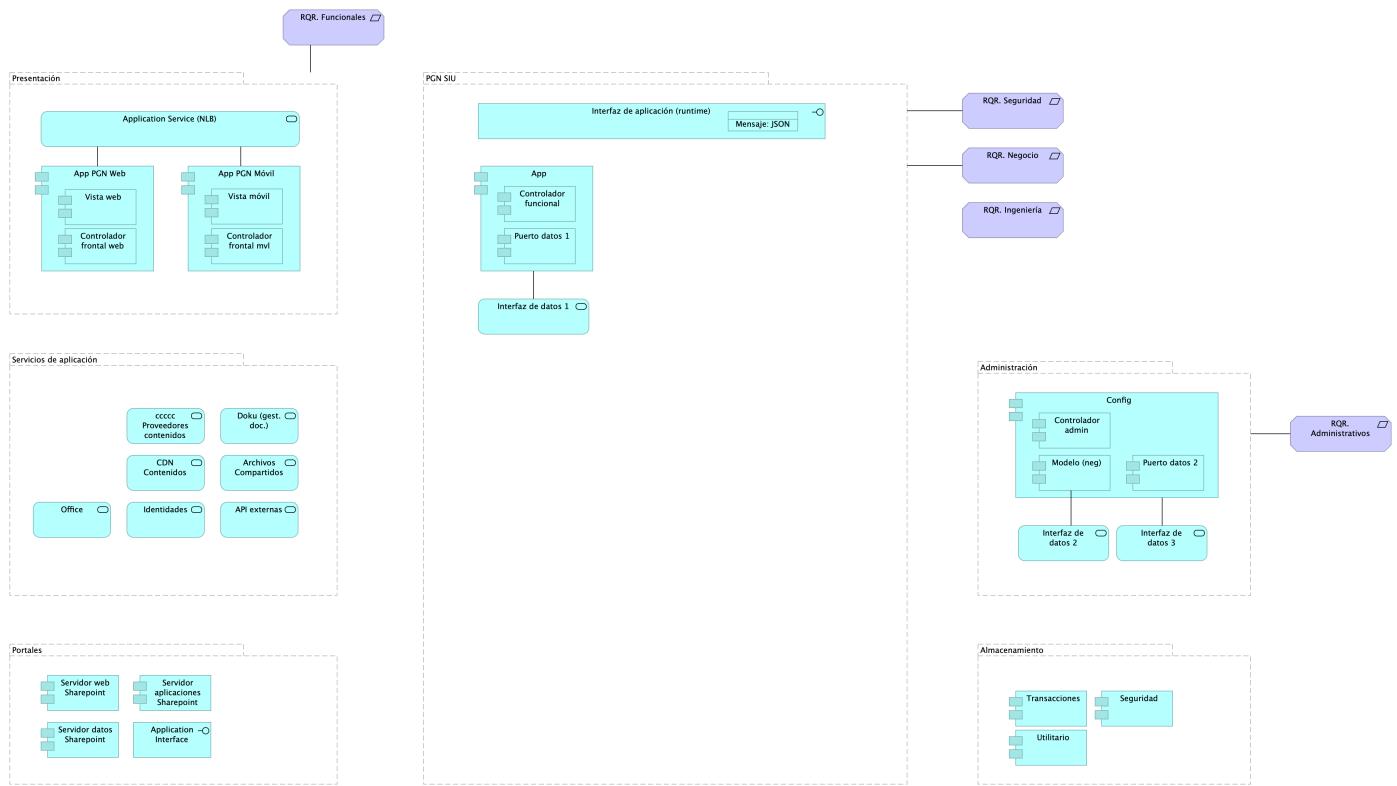


Imagen 55: Seguridad. Migracion.1.SIU modulos

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Nombre	Tipo	Documentación	Propiedad
API externas	Application Service		
Administración	Grouping		
Almacenamiento	Grouping		
App	Application Component		
App PGN Móvil	Application Component	A partir de los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la "Guía de desarrollo OWASP" y "OWAS Cheat Sheet, se realizarán pruebas de seguridad a partir del análisis de vulnerabilidades, y pruebas de Ethikal Hacking.	

Protección de datos personales,

Los sistemas de información que recogen, procesan y almacenan información de los derechos de las personas se deben almacenar de forma adecuada, la información que pueda ser vulnerada puede generar obligaciones legales y éticas con respecto a la pérdida de información confidencial por parte de ciudadanos del país.

La información contenida en las bases de datos debe tener los mecanismos de cifrado que en otros apartados se han mencionado. La legislación que hay que tener como referencia, ley 1581 de 2012. Decreto 1377 de 2013

La metodología empleada tendrá las siguientes fases:

• FASE DE RECONOCIMIENTO:

Se recolectará toda la información posible, usando diferentes técnicas como:

- o Recopilación de dominios/ IPs/puertos/servicios
- o Recopilación de metadatos
- o Uso de Google Dorks.

• ANÁLISIS DE VULNERABILIDADES:

Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.

• EXPLOTACIÓN:

- Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo:
 - Inyección de código
 - Inclusión de ficheros locales o remotos
 - Evasión de autenticación
 - Carencia de controles de autorización
 - Ejecución de comandos en el lado del servidor
 - Ataques tipo Cross Site Request Forgery
 - Control de errores
 - Gestión de sesiones
 - Fugas de información
 - Secuestros de sesión
 - Comprobación de las condiciones para realizar una denegación de servicio.

• POST EXPLOTACIÓN:

En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adicionales con el objetivo de comprobar la criticidad de esta.

No URL IP

1. https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz
135.181.185.207

| | | App PGN Web | Application Component | A partir de los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la "Guía de desarrollo OWASP" y "OWAS Cheat Sheet, se realizarán pruebas de seguridad a partir del análisis de vulnerabilidades, y pruebas de Ethical Hacking.

Los resultados permitirán identificar los requisitos de seguridad que los sistemas de información o servicios web deberán cumplir.
La metodología empleada tendrá las siguientes fases:

• FASE DE RECONOCIMIENTO:

Se recolectará toda la información posible, usando diferentes técnicas como:

- Recopilación de dominios/IPs/puertos/servicios
- Recopilación de metadatos
- Uso de Google Dorks.

• ANÁLISIS DE VULNERABILIDADES:

Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.

• EXPLOTACIÓN:

- Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo:
 - Inyección de código
 - Inclusión de ficheros locales o remotos
 - Evasión de autenticación
 - Carencia de controles de autorización
 - Ejecución de comandos en el lado del servidor
 - Ataques tipo Cross Site Request Forgery
 - Control de errores
 - Gestión de sesiones
 - Fugas de información
 - Secuestros de sesión
 - Comprobación de las condiciones para realizar una denegación de servicio.

• POST EXPLOTACIÓN:

En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adicionales con el objetivo de comprobar la criticidad de esta.

No URL IP

1. https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz
135.181.185.207

El Login deberá evidenciar el control de errores, al momento de realizar la validación deberá mensaje de error para el caso que se autentique con credenciales erradas. | | | Application Interface | Application Interface | | | Application Service (NLB) | Application Service | | | Archivos Compartidos | Application Service | | | CDN Contenidos | Application Service | | | Config | Application Component | | | Controlador admin | Application Component | | | Controlador frontal mvl | Application Component | | | Controlador frontal web | Application Component | - Verificados los SSL, se recomienda adquirir SSL seguros, con entidades certificadoras.

Si se desea continuar con SSL de Let's Encrypt, se recomienda automatizar el proceso de actualización dado que al dejar estos en modo actualización manual es probable el olvido de esta actualización (Estos certificados se deben actualizar trimestralmente y no cuentan con las características de seguridad necesarias).

| | | Controlador funcional | Application Component | | | Doku (gest. doc.) | Application Service | | | Identidades | Application Service | | | Interfaz de aplicación (runtime) | Application Interface | Servidor web: Microsoft-IIS/10.0

Marco de Programación: ASP.NET

Huellas digitales identificadas:

Huella digital SHA-256 "FC:79:06:7E:F5:24:20:50:F1:C0:74:F7:85:56:B9:05:B7:33:A3:2D:44:A0:48"
Huella digital SHA1 "8C:48:BD:E2:F5:18:18:C3:85:96:68:44:2E:28:A0:68:08:2F:0A:BE"

| | | Interfaz de datos 1 | Application Service | | | Interfaz de datos 2 | Application Service | | | Interfaz de datos 3 | Application Service | | | Mensaje: JSON | Data Object | | | Modelo (neg) | Application Component | | | Office | Application Service | | | PGN SIU | Grouping | El objetivo principal de la arquitectura del SUI de la migración es la centralización de los conceptos misionales: concentrar los conceptos misionales en componentes aislados; dejar por fuera de estos componentes misionales todo lo distintos a la misionalidad de la PGN.

Los objetivos secundarios de esta arquitectura SUI de la migración son flexibilidad y extensibilidad. Dichos objetivos son independientes. Es decir, estos pueden ser maximizados sin conflicto entre ellos.

| | | Portales | Grouping | Submódulo de portales internos de la PGN a donde llega el SUI. Interfaz web que usa al SUI para llegar a direcciones y subdirecciones de la PGN. La plataforma principal de portales en este contexto es Sharepoint de Microsoft.
| | | Presentación | Grouping | Submódulo de presentación del SUI. interfaz gráfica, interfaz web visible a los usuarios clientes y funcionarios de la PGN.
| | | Puerto datos 1 | Application Component | | | Puerto datos 2 | Application Component | | | RQR. Administrativos | Requirement | | | RQR. Funcionales | Requirement | | | RQR. Ingeniería | Requirement | | | RQR. Negocio | Requirement | | | RQR. Seguridad | Requirement | Requerimientos de seguridad, SUI, Migración, en aspectos de comunicación, autenticación, autorización y (manejo de) sesiones.
| | | Seguridad | Application Component | | | Servicios de aplicación | Grouping | Submódulo de servicios utilitarios que sirven al SUI. Servicios variados que cumplen roles facilitadores de las actividades misionales del SUI. Ejemplos de estos servicios son los de gestión documental, implementado por Doku en el contexto de PGN.
| | | Servidor aplicaciones Sharepoint | Application Component | | | Servidor datos Sharepoint | Application Component | | | Servidor web Sharepoint | Application Component | | | Transacciones | Application Component | | | Utilitario | Application Component | | | Vista móvil | Application Component | | | Vista web | Application Component | - Verificados los SSL, se recomienda adquirir SSL seguros, con entidades certificadoras.

Si se desea continuar con SSL de Let's Encrypt, se recomienda automatizar el proceso de actualización dado que al dejar estos en modo actualización manual es probable el olvido de esta actualización (Estos certificados se deben actualizar trimestralmente y no cuentan con las características de seguridad necesarias.

4. SERVICIOS IDENTIFICADOS:

Servidor web: Microsoft-IIS/10.0

Marco de Programación: ASP.NET

Huellas digitales identificadas:

Huella digital SHA-256 "FC:79:06:7E:F5:24:20:50:F1:C0:74:F7:85:56:B9:05:B7:33:A3:2D:44:A0:48"

Huella digital SHA1 "8C:48:BD:E2:F5:18:18:C3:85:96:68:44:2E:28:A0:68:08:2F:0A:BE"

| | | cccc Proveedores contenidos | Application Service | | |

Table: Elementos de la vista. {#tbl:tblelement-Seguridad.Migracion.1.SIUmodulos-id}

Seguridad.1. Requerimientos

PGN. Migración Sistemas Misionales. Fase 2.

Submódulos Sistema Único de Información. Requerimientos asociados a submódulos.

versión 0.1

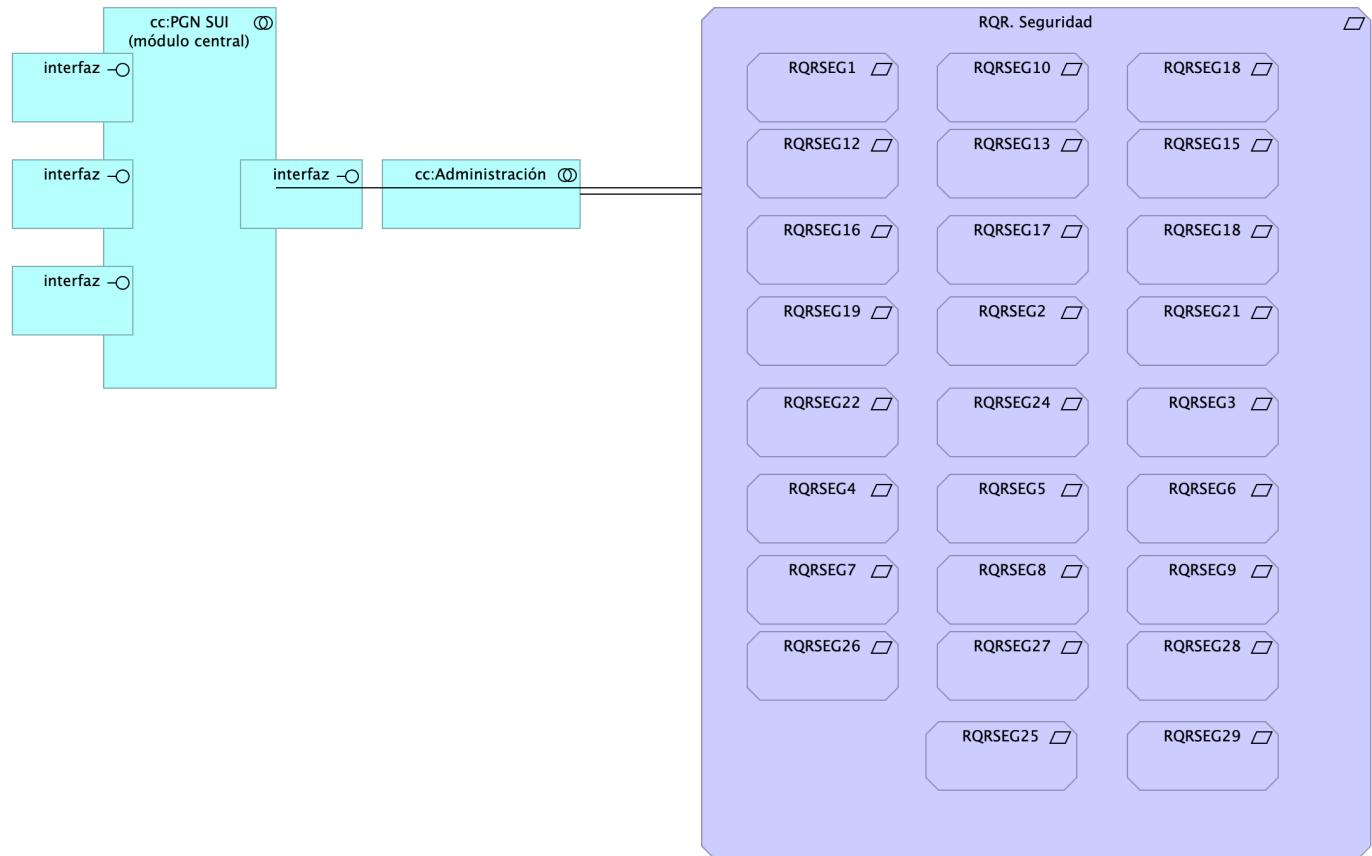


Imagen 56: Seguridad.1. Requerimientos

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Nombre	Tipo	Documentación	Propiedad
RQR. Seguridad	Requirement	Requerimientos de seguridad, SUI, Migración, en aspectos de comunicación, autenticación, autorización y (manejo de) sesiones.	
RQRSEG1	Requirement	1. Las soluciones deben dar cumplimiento a las políticas institucionales del sistema de gestión de seguridad de la información establecidas por la entidad que busca garantizar la confidencialidad, integridad y disponibilidad de la información que se genera, procesa, almacena y/o transmite en los sistemas de Información de la Entidad.	

|| | RQRSEG10 | Requirement | 1. Debe incluir un mecanismo de cifrado de los datos que se transportan entre los diferentes componentes tecnológicos y los datos sensibles de la base de datos que representen un alto nivel de confidencialidad. || | RQRSEG12 | Requirement | 1. Debe contemplar el cumplimiento de la normatividad vigente en cuanto a protección de datos personales y debe permitir el manejo de excepciones.

| | | RQRSEG13 | Requirement | 1. Para los casos que aplique se debe permitir el manejo de certificados y/o firmas digitales en los documentos que así se definan para efectos de aprobación y digitalización. | | | RQRSEG15 | Requirement | 1. Debe funcionar sobre protocolo SSL (certificados internos de la entidad cuando los sistemas de información sean internas y certificados válidos públicamente cuando los sistemas de información estén expuestas a internet). | | | RQRSEG16 | Requirement | 1. Debe entregar un procedimiento para el respaldo de la información de acuerdo con las necesidades de la entidad. | | | RQRSEG17 | Requirement | 1. Debe incluir uso de criptografía para transacciones y/o campos sensibles según lo indiquen las normas vigentes y las necesidades específicas del negocio de acuerdo como lo determine la entidad. | | | RQRSEG18 | Requirement | "1. Debe contemplar un modelo de datos que garantice base de datos única para evitar que se pueda presentar duplicidad de información." | | | RQRSEG18 | Requirement | 1. Debe contemplar un modelo de datos que garantice base de datos única para evitar que se pueda presentar duplicidad de información.,id-d1a6b80e7a6c4538b922f333f4d7ec7a,requirement
RQRSEG11,"1. A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio). | | | RQRSEG19 | Requirement | 1. En la información confidencial solo puede ser consultada por los perfiles autorizados e igualmente restringir documentos de consulta según los privilegios o permisos asociados. | | | RQRSEG2 | Requirement | 1. Las soluciones de automatización de procesos a implementar deben permitir la Gestión de Seguridad de Usuarios, grupos de usuarios y asignación de Roles y perfiles de usuarios, permitiendo asociar las acciones disponibles en la solución con respecto a roles de usuario, permitiendo parametrizar las funcionalidades que cada actor puede usar en la solución. | | | RQRSEG21 | Requirement | 1. Debe cerrar las transacciones luego de máximo 10 minutos de inactividad.""" | | | RQRSEG22 | Requirement | 1. Debe incluir controles de bloqueo de cuenta después de un máximo de 5 intentos erróneos a fin de evitar ataques de fuerza bruta. | | | RQRSEG24 | Requirement | 1. Debe cumplir con todos los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la "Guía de desarrollo OWASP" y "OWAS Cheat Sheet" | | | RQRSEG25 | Requirement | "1. Debe incluir un mecanismo de cifrado de los datos que se transportan entre los diferentes componentes tecnológicos y los datos sensibles de la base de datos que representen un alto nivel de confidencialidad." | | | RQRSEG26 | Requirement | "1. Para los casos que aplique se debe permitir el manejo de certificados o firmas digitales en los documentos que así se definan para efectos de aprobación y digitalización." | | | RQRSEG27 | Requirement | "1. Debe contemplar las prácticas de desarrollo seguro de aplicaciones y/o implementación segura de productos, para su naturaleza Web based." | | | RQRSEG28 | Requirement | "1. A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio)." | | | RQRSEG29 | Requirement | "1. Debe evidenciar el resultado positivo frenteapruebas de ethical hacking, análisis de vulnerabilidades, carga, estrés y desempeño antes de la puesta en operación de acuerdo con los lineamientos de la entidad." | | | RQRSEG3 | Requirement | 1. Un usuario puede estar asociado a uno o más roles, de tal manera que los menús de navegación de la solución se muestran o despliegan dependiendo de las acciones asociadas a cada rol de usuario, permitiendo así que cuando el usuario es autenticado correctamente, la solución verifica los roles que tiene activos para otorgarle únicamente las acciones autorizadas. | | | RQRSEG4 | Requirement | 1. El diseño de la solución debe definir los criterios necesarios para asegurar la trazabilidad y auditoría sobre las acciones de creación, actualización, modificación o borrado de los componentes de información, de tal manera que la solución debe permitirle al administrador de la solución parametrizar las tablas y eventos que pueden auditarse. | | | RQRSEG5 | Requirement | 1. Las soluciones deben tener en cuenta mecanismos que aseguren el registro histórico para poder mantener la trazabilidad de las acciones realizadas por los usuarios, contemplando el registro de auditoría que contiene información de fecha y hora, identificación del registro, tabla afectada, descripción del evento, tipo de evento, usuario que realiza la acción, identificación de sesión y dirección IP del usuario que efectuó la transacción. | | | RQRSEG6 | Requirement | 1. La solución debe proveer una consulta que permita a un usuario con los privilegios asignados, consultar los registros de auditoría, aplicando criterios de filtro (usuario, máquina, rango de fechas y tipo de operación). | | | RQRSEG7 | Requirement | 1. Las soluciones deben integrarse con LDAP – (Lightweight Directory Access Protocol) para los procesos de inicio de sesión y autenticación. La solución debe soportar la integración Nativa con Active Directory de Microsoft. Para usuarios externos el mecanismo de autorización, autenticación y acceso será controlado a través del modelo de seguridad de la solución (no habrá autenticación para usuarios externos). | | | RQRSEG8 | Requirement | 1. Las soluciones deben cumplir con los lineamientos de seguridad relacionados a su utilización a través de redes públicas y privadas, garantizando la confidencialidad e integridad de la información y acceso a ella. | | | RQRSEG9 | Requirement | 1. Debe evidenciar que, a través de pruebas de vulnerabilidad, garantiza la seguridad de la información. Estas pruebas deben suministrar evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad. | | | cc:Administración | Application Collaboration | | | cc:PGN SUI (módulo central) | Application Collaboration | Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN.
| | | interfaz | Application Interface | | |

Table: Elementos de la vista. {#tbl:tblelement-Seguridad.1.Requerimientos-id}

Seguridad.2. Lineabase.0.SIU Application

2MFA

Representación Arquitectónica

Con una arquitectura orientada a servicios SUI recopila:

1. Runtime: Es el servicio que interactúa con el usuario final (GUI) elaborado en Angular 11
2. API Tx: Servicio api rest base node encargado de realizar las transacciones básicas CRUD
3. API Config / Seguridad. Servicio Web API .Net Framework encargado de gestionar características con la autenticación y configuración

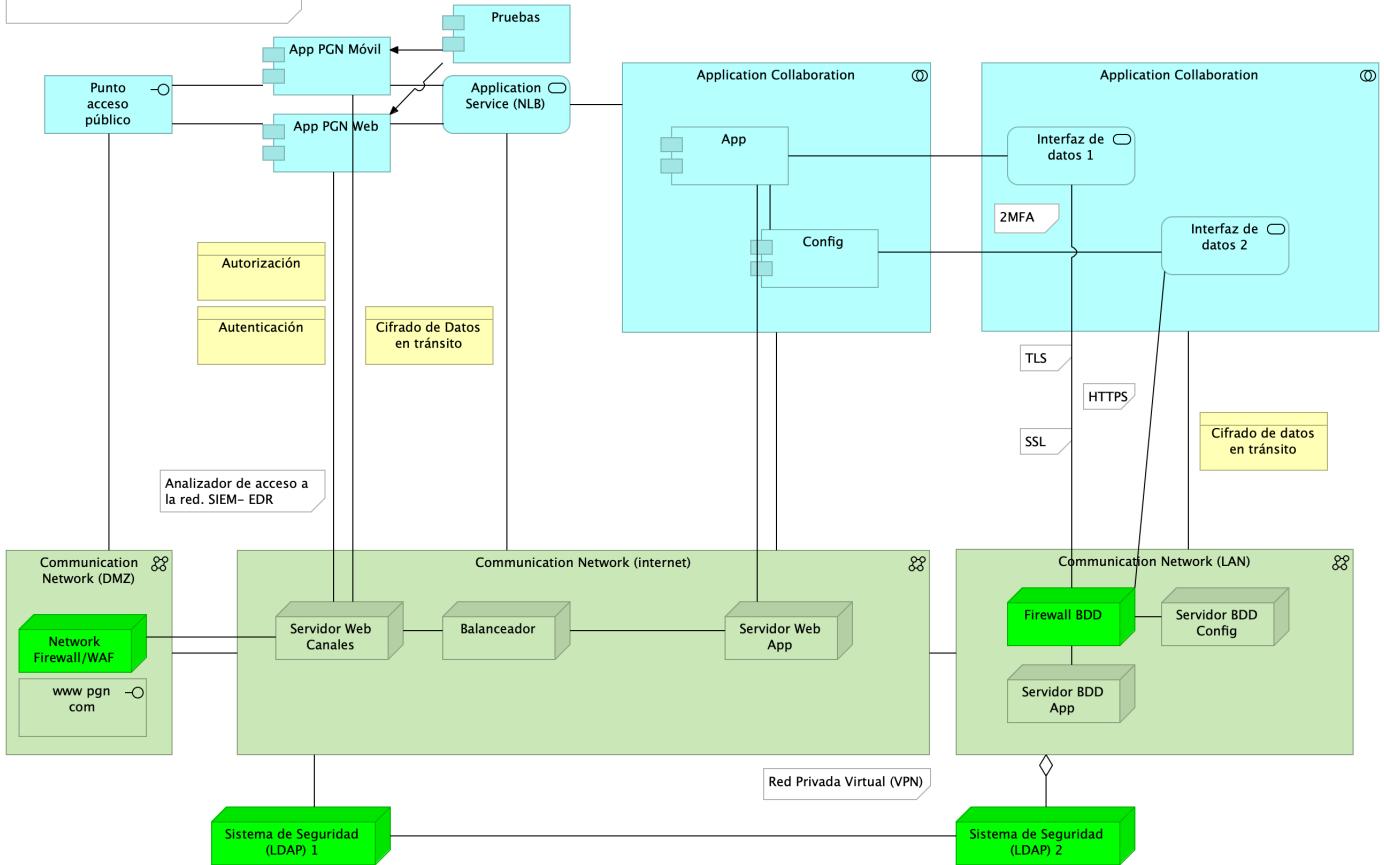


Imagen 57: Seguridad.2. Lineabase.0.SIU Aplicación

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Nombre	Tipo	Documentación	Propiedad
App	Application Component		
App PGN Móvil	Application Component	A partir de los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la "Guía de desarrollo OWASP" y "OWAS Cheat Sheet, se realizarán pruebas de seguridad a partir del análisis de vulnerabilidades, y pruebas de Ethikal Hacking.	

Protección de datos personales,

Los sistemas de información que recogen, procesan y almacenan información de los derechos de las personas se deben almacenar de forma adecuada, la información que pueda ser vulnerada puede generar obligaciones legales y éticas con respecto a la pérdida de información confidencial por parte de ciudadanos del país.

La información contenida en las bases de datos debe tener los mecanismos de cifrado que en otros apartados se han mencionado.
La legislación que hay que tener como referencia, ley 1581 de 2012. Decreto 1377 de 2013

La metodología empleada tendrá las siguientes fases:

- **FASE DE RECONOCIMIENTO:**
Se recolectará toda la información posible, usando diferentes técnicas como:
 - o Recopilación de dominios/IPs/puertos/servicios
 - o Recopilación de metadatos
 - o Uso de Google Dorks.

- **ANÁLISIS DE VULNERABILIDADES:**

Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.

• EXPLOTACIÓN:

- Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo:
 - Inyección de código
 - Inclusión de ficheros locales o remotos
 - Evasión de autenticación
 - Carencia de controles de autorización
 - Ejecución de comandos en el lado del servidor
 - Ataques tipo Cross Site Request Forgery
 - Control de errores
 - Gestión de sesiones
 - Fugas de información
 - Secuestros de sesión
 - Comprobación de las condiciones para realizar una denegación de servicio.

• POST EXPLOTACIÓN:

En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adicionales con el objetivo de comprobar la criticidad de esta.

No URL IP

1. https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz
135.181.185.207

| | | App PGN Web | Application Component | A partir de los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la "Guía de desarrollo OWASP" y "OWAS Cheat Sheet", se realizarán pruebas de seguridad a partir del análisis de vulnerabilidades, y pruebas de Ethical Hacking.

Los resultados permitirán identificar los requisitos de seguridad que los sistemas de información o servicios web deberán cumplir.
La metodología empleada tendrá las siguientes fases:

• FASE DE RECONOCIMIENTO:

Se recolectará toda la información posible, usando diferentes técnicas como:

- Recopilación de dominios/IPs/puertos/servicios
- Recopilación de metadatos
- Uso de Google Dorks.

• ANÁLISIS DE VULNERABILIDADES:

Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.

• EXPLOTACIÓN:

- Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo:
 - Inyección de código
 - Inclusión de ficheros locales o remotos
 - Evasión de autenticación
 - Carencia de controles de autorización
 - Ejecución de comandos en el lado del servidor
 - Ataques tipo Cross Site Request Forgery
 - Control de errores
 - Gestión de sesiones
 - Fugas de información
 - Secuestros de sesión
 - Comprobación de las condiciones para realizar una denegación de servicio.

• POST EXPLOTACIÓN:

En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adicionales con el objetivo de comprobar la criticidad de esta.

No URL IP

1. https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz
135.181.185.207

El Login deberá evidenciar el control de errores, al momento de realizar la validación deberá mensaje de error para el caso que se autentique con credenciales erradas. | | | Application Collaboration | Application Collaboration | | | Application Collaboration | Application Collaboration | | | Application Service (NLB) | Application Service | | | Autenticación | Business Object | Con el objetivo de incrementar el nivel de seguridad, para el proceso de autenticación se tendrán en cuenta las siguientes consideraciones:

Validación del proceso de gestión de usuarios: La fortaleza de la autenticación dependerá del proceso de gestión de usuarios implementado por parte de la entidad. Se debe tener en cuenta los lineamientos definidos en la política Específica de Control de Acceso.

Autenticación con integración de Windows: La autenticación permitirá que los usuarios asignados al dominio, una vez que se ingresen las credenciales, y realizada la validación, se autorizará el acceso a los servicios y/o soluciones a partir de la integración del directorio activo con la integración del LDAP – (Lightweight Directory Access Protocol).

Los tipos de autenticación realizadas a partir de las identidades administradas de los recursos de Azure, entidades de Servicio y Certificados, podrán ser integrado con los dominios del directorio activo (DA) local. Por lo que respecta a la autenticación, será generado con la asignación de usuarios y credenciales definidas alineadas con la política Específica de Control de Acceso., a partir de la integración será validado el ingreso a las diferentes soluciones y/o sistemas de información de la PGN.

Manejo y uso de contraseñas: Los servidores públicos deberán tener en cuenta los lineamientos definidos para la creación y gestión de contraseñas del Sistema de Gestión de Seguridad de la Información SGSI de la Procuraduría General de la Nación.

Utilización de canales cifrados: El proceso de autenticación tendrá mecanismos de transmisión seguro. El uso del TLS (Transport Layer Security), será necesario para el acceso a la página de autenticación que ayude a garantizar la autenticidad de la aplicación a los funcionarios, como en la transmisión de las credenciales.

Bloqueo de cuentas: Aquellas cuentas sobre las que se han realizado múltiples intentos de conexiones fallidas, cinco (5) intentos erróneos, se tendrá implementado un bloqueo temporal o permanente como mecanismo de seguridad para evitar amenazas de ataques. | | | Autorización | Business Object | Metodología

Los mecanismos de autorización para el acceso a los sistemas de información de la procuraduría general de la nación describen la forma de cómo se restringe el acceso a los diferentes módulos (Misionales (SIM), Registros de Inhabilidades (SIRI), Nómina, Control Interno y relatoría, entre otros.), y que se considera un mecanismo de protección, que ayuda a reaccionar ante cualquier operación no autorizada. El control de acceso basado en roles (RBAC), enfoca la idea de que a los funcionarios se les otorgue los permisos de acceso a los recursos, basados en los roles y/o perfiles que este posee. Este control posee dos características fundamentales: i) los accesos son controlados por medio de los roles y/o perfiles asignados, quiere decir, a los servidores públicos, contratistas, terceros y otros colaboradores autorizados para interactuar con los sistemas de información se le asignan los roles y el encargado/responsable definirá los permisos, que a su vez están relacionados con los roles, ii) Los roles pueden ser definidos a nivel jerárquico, es decir que un rol podrá ser miembro de otro rol.

Un proceso de autorización basado en roles, identifica tres factores importantes, i) Todos los servidores públicos, contratistas, terceros y otros Colaboradores, deben tener un rol asignado, si no es asignado no podrá realizar ninguna acción relacionada con el acceso, ii) un usuario podrá hacer uso de los permisos asociados a los roles asignados, el cual deberá realizar el inicio de sesión el usuario asignado del Directorio activo (DA), iii) los servidores públicos, contratistas, terceros y otros, solo podrán realizar acciones para las cuales han sido autorizados por medio de la activación de sus roles y/o perfiles.

EL control definido para los accesos basados en roles RBAC, permitirá que solo las personas autorizadas de la PGN podrán acceder a ciertos recursos (programas, equipos, aplicaciones, bases de datos, etc.) definido por sus funciones laborales, lo que permitirá controlar los accesos desde diferentes escenarios: Sistemas de información, redes y aplicaciones.

Gestión de identidades y Control de acceso:

Gestor de identidades: En esta gestión se planifica el ciclo de vida de las identidades de usuario y se realizan los procesos de sincronización, de acuerdo a los suministros de accesos establecidos por la entidad, los cuales son integrados con el servidor que gestiona la identidad y control de acceso.

Gestor de roles: La asignación de roles es sincronizada con la identidad de usuario en el servidor de dominio. Para esta gestión se crean las reglas y condiciones que determinan si un usuario puede o no pertenecer a un rol definido por la entidad.

Para el gobierno y gestión de identidades y de acceso, se identificó como primera medida la implementación de la siguiente metodología.

REGLAS PARA LA CREACIÓN DE USUARIOS.

Identificación de Mecanismos:

En este ítem se deben identificar las herramientas con las que cuenta la entidad, las cuales deberán ser registradas en el documento denominado: "Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_1 (Mecanismos)".

Identificación de Roles y Privilegios

Este ítem proporciona al sistema la definición de las políticas organizacionales en cuanto a la definición de los privilegios y roles de los diferentes actores en cada uno de los aplicativos con los que estos interactúan dentro de sus funciones, registradas en el documento denominado: "Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_2 (Roles)".

Aprovisionamiento de cuentas

Este ítem establece el proceso adecuado para el aprovisionamiento y des aprovisionamiento de cuentas de usuarios en las diferentes aplicaciones, permitiendo toda la gestión de ellas por medio de un sistema de directorio único y centralizado, Este aprovisionamiento se encuentra registrado en el documento denominado: "Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_4 y Hoja_5 (Permisos)".

Establecimiento de mecanismos de control de acceso:

Este ítem controla que usuarios tienen permitido el acceso a los diferentes aplicativos o herramientas dentro de la organización permitiendo separar las funciones dependiendo del rol del usuario en cada sistema, Este establecimiento se encuentra registrado en el documento denominado: "Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_3 (Acceso)".

Definición de Privilegios y accesos.

Los accesos y privilegios serán identificados en la matriz, encargado identificar cada uno de los roles y perfiles que se tendrá cada usuario hacia los

sistemas de información cumpliendo con el principio del menor privilegio, teniendo en cuenta que los usuarios deberán tener exclusivamente los permisos y privilegios que necesita para el desarrollo de sus actividades. La matriz identificará i) los roles que se deben crear para cada sistema de información, ii) los privilegios que requiere cada rol del sistema y iii) los niveles de accesos requeridos, (Consultar, Modificar, Eliminar) (CRUD) y iv) Tipos de usuarios, roles que pueden ser asignados al perfil, entre otros.

Configuración de permisos

La configuración con de los perfiles con sus accesos y privilegios en los sistemas de información se debe realizar empleando las herramientas propias de la procuraduría general de la nacional PGN, y serán asignados los permisos según la matriz de roles y permisos.

Identificación de Mecanismos:

En este ítem se deben identificar las herramientas con las que cuenta la entidad, las cuales deberán ser registradas en el documento denominado: "Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_1 (Mecanismos)".

Identificación de Roles y Privilegios

Este ítem proporciona al sistema la definición de las políticas organizacionales en cuanto a la definición de los privilegios y roles de los diferentes actores en cada uno de los aplicativos con los que estos interactúan dentro de sus funciones, registradas en el documento denominado: "Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_2 (Roles)".

Aprovisionamiento de cuentas

Este ítem establece el proceso adecuado para el aprovisionamiento y des aprovisionamiento de cuentas de usuarios en las diferentes aplicaciones, permitiendo toda la gestión de ellas por medio de un sistema de directorio único y centralizado, Este aprovisionamiento se encuentra registrado en el documento denominado: "Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_4 y Hoja_5 (Permisos)".

Establecimiento de mecanismos de control de acceso:

Este ítem controla que usuarios tienen permitido el acceso a los diferentes aplicativos o herramientas dentro de la organización permitiendo separar las funciones dependiendo del rol del usuario en cada sistema, Este establecimiento se encuentra registrado en el documento denominado: "Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_3 (Acceso)".

Definición de Privilegios y accesos.

Los accesos y privilegios serán identificados en la matriz, encargado identificar cada uno de los roles y perfiles que se tendrá cada usuario hacia los sistemas de información cumpliendo con el principio del menor privilegio, teniendo en cuenta que los usuarios deberán tener exclusivamente los permisos y privilegios que necesita para el desarrollo de sus actividades. La matriz identificará i) los roles que se deben crear para cada sistema de información, ii) los privilegios que requiere cada rol del sistema y iii) los niveles de accesos requeridos, (Consultar, Modificar, Eliminar) (CRUD) y iv) Tipos de usuarios, roles que pueden ser asignados al perfil, entre otros.

Configuración de permisos

La configuración con de los perfiles con sus accesos y privilegios en los sistemas de información se debe realizar empleando las herramientas propias de la procuraduría general de la nacional PGN, y serán asignados los permisos según la matriz de roles y permisos. | | | Balanceador | Node | | | Cifrado de Datos en tránsito | Business Object | Proteger la información propia de la PGN utilizando mecanismos de cifrado que permita garantizar los pilares de Seguridad de la Información Confidencialidad e integridad, asimismo reducir los riesgos de la información mediante la ayuda de Técnicas Criptográficas.

Como mecanismos se propone implementar estos mecanismos de cifrado, como el protocolo TLS (Transport Layer Security) que permite a dos partes identificarse y autenticarse entre sí y comunicarse con confidencialidad e integridad de datos a partir de la conexión del usuario y un servidor WEB.

Se propone integrar certificados SSL, que permite cifrar la información confidencial a fin de que solo los autorizados puedan tener acceso a ella, y así evitar manipulación de información confidencial. La Seguridad que brinda SSL, da garantía para acceder a los aplicativos de PNG.

Como implementar certificados SSL?

Podrán ser adquiridos a través del proveedor de dominios.

TLS es el protocolo que surge para reforzar la seguridad de los certificados SSL, que funciona como mecanismo de encriptación para que sea realmente transparente el envío de la información, proporcionando una autenticación sólida, restringiendo la manipulación, interceptación y alteración de mensajes.

La última versión del TLS es la 1.3

| | | Cifrado de datos en tránsito | Business Object | Proteger la información propia de la PGN utilizando mecanismos de cifrado que permita garantizar los pilares de Seguridad de la Información Confidencialidad e integridad, asimismo reducir los riesgos de la información mediante la ayuda de Técnicas Criptográficas. Como mecanismos se propone implementar estos mecanismos de cifrado, como el protocolo TLS (Transport Layer Security) que permite a dos partes identificarse y autenticarse entre sí y comunicarse con confidencialidad e integridad de datos a partir de la conexión del usuario y un servidor WEB.

Se propone integrar certificados SSL, que permite cifrar la información confidencial a fin de que solo los autorizados puedan tener acceso a ella, y así evitar manipulación de información confidencial. La Seguridad que brinda SSL, da garantía para acceder a los aplicativos de PNG.

Como implementar certificados SSL?

Podrán ser adquiridos a través del proveedor de dominios.

TLS es el protocolo que surge para reforzar la seguridad de los certificados SSL, que funciona como mecanismo de encriptación para que sea realmente transparente el envío de la información, proporcionando una autenticación sólida, restringiendo la manipulación, interceptación y alteración de mensajes.

La última versión del TLS es la 1.3 | | | Communication Network (DMZ) | Communication Network | | | Communication Network (LAN) | Communication Network | | | Communication Network (internet) | Communication Network | | | Config | Application Component | | | Firewall BDD | Node | | | Interfaz de datos 1 | Application Service | | | Interfaz de datos 2 | Application Service | | | Network Firewall/WAF | Node | | |

Pruebas | Application Component | FASE DE RECONOCIMIENTO:

Se recolectará toda la información posible, usando diferentes técnicas como:

Recopilación de dominios/IPs/puertos/servicios

Recopilación de metadatos

Uso de Google Dorks.

ANÁLISIS DE VULNERABILIDADES:

Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.

EXPLOTACIÓN:

Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo:

Inyección de código

Inclusión de ficheros locales o remotos

Evasión de autenticación

Carencia de controles de autorización

Ejecución de comandos en el lado del servidor

Ataques tipo Cross Site Request Forgery

Control de errores

Gestión de sesiones

Fugas de información

Secuestros de sesión

Comprobación de las condiciones para realizar una denegación de servicio.

POST EXPLOTACIÓN:

En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adicionales con el objetivo de comprobar la criticidad de esta. | | | Punto acceso público | Application Interface | URL tipo C

HTTP | | | Servidor BDD App | Node | Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz

Discos SO C: 126 GB, Backup E: 511 GB, SQL Data F: 510 GB, SQL Log G: 510 GB, TempDB G: 63.6 GB.

| | | Servidor BDD Config | Node | Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz

Discos SO C: 80 GB, Backup E: 250 GB, SQL Data F: 250 GB, SQL Log G: 250 GB, TempDB G: 30 GB.

| | | Servidor Web App | Node | Windows Server 2019 Standard o Datacenter x64. Nombre físico. IP LAN. IP Pública. Windows Server 2019 Standard or Datacenter x64. RAM 8 GB. CPU 64 Bits. 4 Cores de 2 Ghz. Discos SO C: 126 GB. SO D: 16 GB.

| | | Servidor Web Canales | Node | Windows Server 2019 Standard o Datacenter x64. Nombre físico. IP LAN. IP Pública. Windows Server 2019 Standard or Datacenter x64. RAM 8 GB. CPU 64 Bits. 4 Cores de 2 Ghz. Discos SO C: 126 GB. SO D: 16 GB.

| | | Sistema de Seguridad (LDAP) 1 | Node | Sistema de Seguridad (LDAP) 1. Control de acceso internet,

La autenticación podrá estar integrada con el directorio activo, a partir de la generación de código para el ingreso con 2FA, que podrá generar un código la plataforma de correo corporativo, el cual solicitará el código de autenticación y una vez ingresado podrá redirigir al sitio.

| | | Sistema de Seguridad (LDAP) 2 | Node | Sistema de Seguridad (LDAP) 2. Control de acceso internet,

La solución se podrá integrar con el directorio activo, a partir de la generación del 2FA, que podrá generar un código por la plataforma de Office 365, el cual solicitará el código de autenticación y una vez ingresado podrá acceder al sitio.

| | | www.pgn.com | Technology Interface | | |

Table: Elementos de la vista. {#tbl:tblelement-Seguridad.2.Lineabase.0.SIUAplicación-id}

Seguridad.3. Datos SUI

undefined

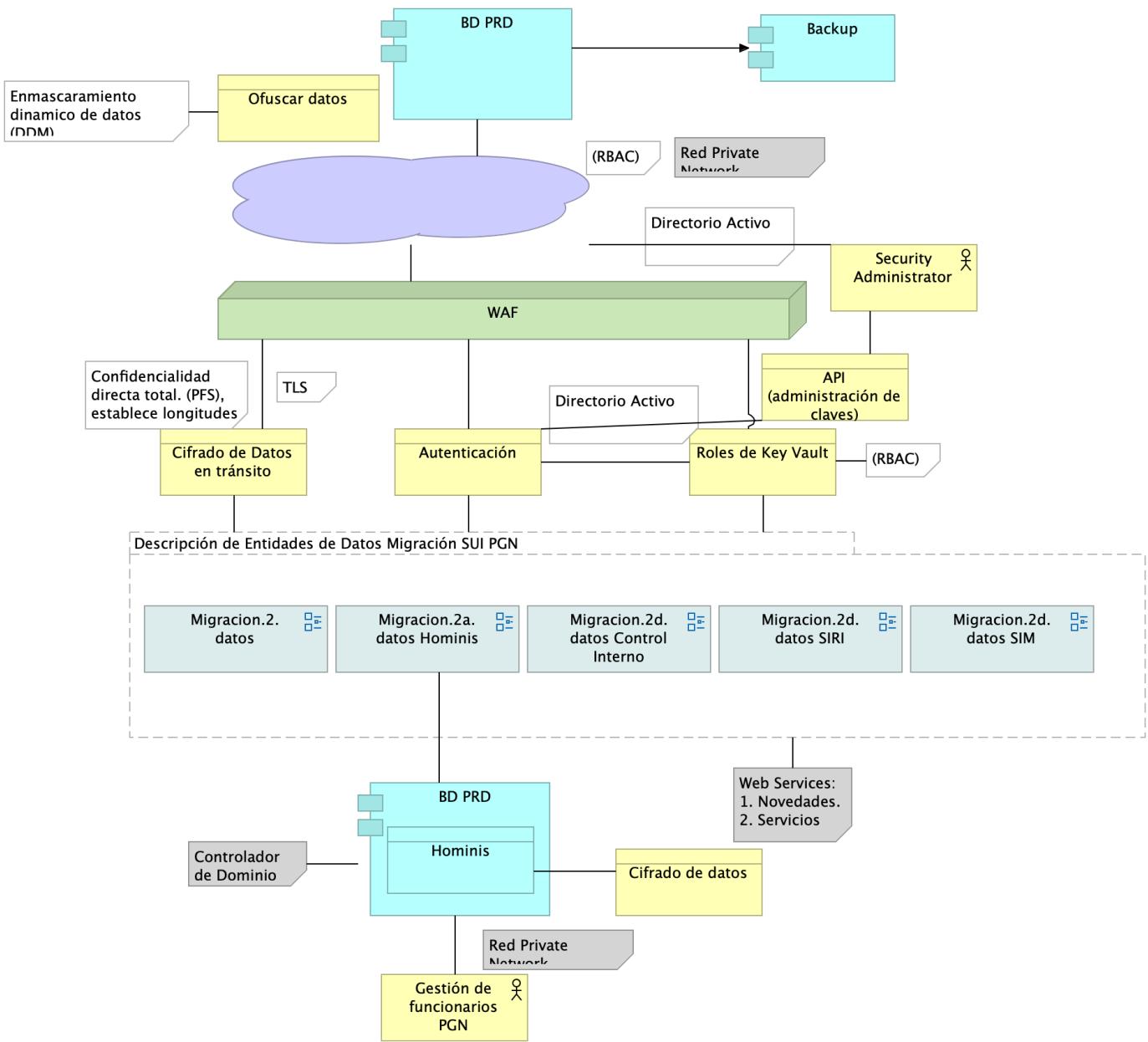


Imagen 58: Seguridad.3. Datos SUI

Fuente: Repositorio arquitectura Mi Mutual (2023)

Catálogo de Elementos

Nombre	Tipo	Documentación	Propiedad
	Meaning		
API (administración de claves)	Business Object	Administración de claves.	
Las contraseñas deberán cumplir con los requisitos de complejidad y completitud, teniendo en cuenta la longitud, caracteres numéricos, alfabéticos y especiales y que puedan ser cambiadas en un periodo de tiempo establecido, de acuerdo con los parámetros definidos en las políticas de acceso.			
Autenticación	Business Object	Los tipos de autenticación realizadas a partir de las identidades administradas de los recursos de Azure, entidades de Servicio y Certificado y entidad de servicio secreto, podrán ser integrado con los dominios del DA locales.	

Por lo que respecta a la autenticación, será generado con la (Validación de nombre de usuario y contraseñas proporcionadas por el funcionario), a partir

de la integración del directorio activo LDAP. Con la aceptación del usuario y contraseñas, se podrán ingresar a los diferentes sistemas de información de la PGN.

Se definirá política dentro del directorio activo DA para que los usuarios que ingresen su contraseña de forma errónea, se bloquee automáticamente, así mismo la política para el bloqueo de los usuarios desatendidos después de dos (2) minutos de inactividad. | | | BD PRD | Application Component | Gestor de Base de datos SQL Server.

Permitirá enmascarar los datos a nivel de columna, teniendo en cuenta el enmascaramiento dinámico de datos (DDM).

Se podrá utilizar el mecanismo de cifrado a nivel de columna para almacenar los datos confidenciales en formato de cifrado.

Para el cifrado de los datos en columna se podrá tener en cuenta las funciones de cifrado (ENCRYPT_AES() y ENCRYPT_TDES()), parámetros que se incorporan para cifrar los datos que contengan datos de tipo Varchar, Caracter entre otros.

para la protección de datos en filas de bases de datos, se tendrá en cuenta mediante la instrucción transact-SQL CREATE SECURITY POLICY. | | | Backup | Application Component | Para el respaldo de las bases de datos en los ecosistemas de Dev, Test, Prod se cuenta con las siguientes políticas de retención de copias de seguridad y frecuencia de copias de seguridad.

Para la base de datos de seguridad y configuración de la aplicación se tiene un plan de copia completa cada 12 horas (PITR) en una franja de tiempo de 35 días. Adicionalmente cuenta con un LTR de conservación de 12 semanas para las copias de seguridad semanales, 12 semanas de conservación para la primera copia de seguridad de cada mes, y una conservación de 12 semanas de una copia de seguridad anual.

Para la base de datos de datos y trazabilidad de transacciones de la aplicación se tiene un plan de copia completa cada 12 horas (PITR) en una franja de tiempo de 35 días. Adicionalmente cuenta con un LTR de conservación de 52 semanas para copias de seguridad semanales, 52 semanas de conservación para la primera copia de seguridad de cada mes, y una conservación de 52 semanas de una copia de seguridad anual. Esto con la finalidad de que al ser una base de datos transaccional precisa de una conservación completa de los años transaccionales. | | | Cifrado de Datos en tránsito | Business Object | Proteger la información propia de la PGN utilizando mecanismos de cifrado que permita garantizar los pilares de Seguridad de la Información Confidencialidad e integridad, asimismo reducir los riesgos de la información mediante la ayuda de Técnicas Criptográficas.

Como mecanismos se propone implementar estos mecanismos de cifrado, como el protocolo TLS (Transport Layer Security) que permite a dos partes identificarse y autenticarse entre sí y comunicarse con confidencialidad e integridad de datos a partir de la conexión del usuario y un servidor WEB.

Se propone integrar certificados SSL, que permite cifrar la información confidencial a fin de que solo los autorizados puedan tener acceso a ella, y así evitar manipulación de información confidencial. La Seguridad que brinda SSL, da garantía para acceder a los aplicativos de PNG.

Como implementar certificados SSL?

Podrán ser adquiridos a través del proveedor de dominios.

TLS es el protocolo que surge para reforzar la seguridad de los certificados SSL, que funciona como mecanismo de encriptación para que sea realmente transparente el envío de la información, proporcionando una autenticación sólida, restringiendo la manipulación, interceptación y alteración de mensajes.

La última versión del TLS es la 1.3

| | | Cifrado de datos | Business Object | Establecer mecanismos de cifrado, como el protocolo TLS (Transport Layer Security) que permite a dos partes identificarse y autenticarse entre sí y comunicarse con confidencialidad e integridad de datos a partir de la conexión del usuario y un servidor WEB. | | | Descripción de Entidades de Datos Migración SUI PGN | Grouping | | | Gestión de funcionarios PGN | Business Actor | La autenticación de usuarios estará enmarcada en tres factores de autenticación a partir del controlador de Dominio, y el acceso por VPN. | | | Hominis | Data Object | | | Ofuscar datos | Business Object | Permitirá enmascarar los datos a nivel de columna, teniendo en cuenta el enmascaramiento dinámico de datos (DDM). Se podrá utilizar el mecanismo de cifrado a nivel de columna para almacenar los datos confidenciales en formato de cifrado.

Para el cifrado de los datos en columna se podrá tener en cuenta las funciones de cifrado (ENCRYPT_AES() y ENCRYPT_TDES()), parámetros que se incorporan para cifrar los datos que contengan datos de tipo Varchar, Caracter entre otros.

para la protección de datos en filas de bases de datos, se tendrá en cuenta mediante la instrucción transact-SQL CREATE SECURITY POLICY. | | | Roles de Key Vault | Business Object | Control de acceso que define los roles y los privilegios para determinar si a un usuario se le debe dar acceso a un recurso.

La información que sea considerada como Información pública reservada de acuerdo con los criterios definidos en la ley 1712 de 2014 "Por medio del cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional.", podrá ser consultada solo por el personal autorizado definido de acuerdo con el control de acceso basado en roles. Los perfiles o roles definirán el acceso a la información.

Para los documentos restringidos que requieran firma por parte del líder del proceso o propietario, se propone revisar la implementación de un dispositivo criptográfico con uso de (CERTIFICADOS y FIRMA DIGITAL) con token integrado que podrá ser conectado en el puerto USB de la máquina del usuario.

La aprobación de los documentos por intermedio de esta firma permitirá la aprobación, integridad de los documentos, seguridad y validez jurídica. Se propone la gestión con un proveedor de certificado del ámbito nacional.

El control definido para los accesos basados en roles RBAC, permitirá que solo las personas autorizadas de la PGN podrán acceder a ciertos recursos (programas, equipos, aplicaciones, bases de datos, etc) definido por sus funciones laborales, lo que permitirá controlar los accesos desde diferentes escenarios: Sistemas de información, redes y aplicaciones. | | | Security Administrator | Business Actor | La autenticación de usuarios estará enmarcada en tres factores de autenticación:

control de acceso basado en roles (RBAC), mecanismo de control de acceso que define los roles y los privilegios para determinar si a un usuario se le debe dar acceso a un recurso.

Conexión de acceso por DA de Azure: Servicio de administración de acceso e identidades basado en la nube.

Red Privada Virtual de Azure: bloqueo de compilación fundamental para las redes privadas en Azure | | | WAF | Node | El WAF es la medida de implementación del muro de protección (firewall) de Aplicaciones WEB del SUI necesario para el control de las peticiones realizadas desde fuera del perímetro de red y hacia los sistemas de información de la PGN.

| |

Table: Elementos de la vista. {#tbl:tblelement-Seguridad.3.DatosSUI-id}

Vistas de Arquitectura Cotizador

- [Cotizador Web](#)
 - [ArqCotizador. 1. Contexto](#)
 - [ArqCotizador. 2. Contenedores](#)
 - [ArqCotizador. 4. Aplicación](#)

- [ArqCotizador. 4a. Aplicación. Servicios](#)
- [ArqCotizador. 4a. Dependencias](#)
- [ArqCotizador. 5. Físico \(despliegue\)](#)
- [ArqCotizador. 7. Datos. Negocio](#)

Cotizador Web

ArqCotizador. 1. Contexto

Mi Mutual. Coomeva, 2023.
Cotizador Web Mi Mutual. Contexto
Mi Mutual: Áreas negocio,
componente central Mi Mutual,
servicios y funciones.
versión 0.1

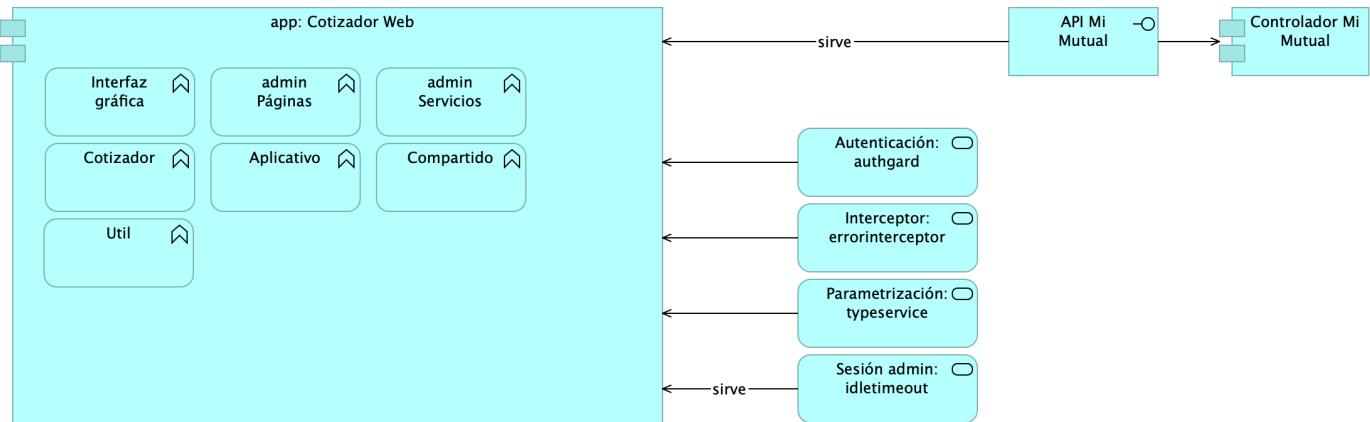


Imagen 59: Diagrama: ArqCotizador. 1. Contexto

Contexto Mi Mutual Web

La aplicación Cotizador Web hace parte de los módulos de interfaz web de Mi Mutual Central, representado por API Mi Mutual en el diagrama. Realizar cotizaciones de los planes de protección luego de la vinculación del asociado.

La estructura por módulos permite realizar aplicaciones escalables y robustas ya que permite organizar las partes de la aplicación, la organización en bloques, extender la aplicación con funcionalidades de librerías externas, proporcionar un entorno de resolución de plantillas y además permite especificar la forma de la carga de cada uno de los componentes y servicios que conforman un módulo.

Módulos Externos

Los módulos externos son todas y cada uno de las herramientas que se utilizan para complementar con funcionalidades ya desarrolladas y tomadas desde un repositorio externo (NPM).

- TranslateModule: Manejo de internacionalización. Documentación: <https://github.com/ngx-translate/core>
- NgxMaskModule: Manejo de máscaras de input text. Documentación: <https://github.com/JsDaddy/ngx-mask>
- JwtModule: Manejo de token. Documentación: <https://github.com/auth0/angular2-jwt>
- sweetalert2: Manejo de alertas de mensajes. Documentación: <https://sweetalert2.github.io/>
- ngx-ui-loader: Manejo de Spinner para control de peticiones asíncronas. Documentación: <https://github.com/t-ho/ngx-ui-loader>
- Ngprime: Manejo de componentes visuales Documentación: <https://www.primefaces.org/primeng/#/>
- chart.js: componente utilizado para el manejo de graficas Documentación: <https://www.chartjs.org/docs/latest/>
- classlist.js: componente para el manejo de listas de datos en las gráficas Documentación: <https://www.chartjs.org/docs/latest/>
- crontrue: componente para traducir una expresión cron a palabras Documentación: <https://github.com;bradymholt/crontrue>
- file-saver: componente para descargar un archivo desde los bytes Documentación: <https://github.com/eligrey/FileSaver.js#readme>
- ngx-tinymce: Editor html para generación de plantillas para cartas Documentación: <https://cipchk.github.io/ngx-tinymce/#/>
- quill: componente para editor html Documentación: <https://quilljs.com/>

Servicios Transversales

- AuthGuard: Validación de existencia de autenticación
- DeactiveGuard: Validación de salida de un componente
- ErrorInterceptor: Interceptor de Errores del back
- JwtInterceptor: Interceptor para injectar el token
- AuthenticationService: Métodos para completar la autenticación
- TypesService: Consumo de servicios de parametrización
- IdleTimeoutService: Verificación de timeout del token

Catálogo de Elementos

Name	Type	Description	Properties
------	------	-------------	------------

Name	Type	Description	Properties
Controlador Mi Mutual	application-component	Los componentes de este tipo se encargan de controlar los servicios rest de la aplicación, además en estos componentes se define la forma como se reciben y envían los datos de los servicios rest y la seguridad de cada uno de los métodos.	<i>modulo: mimutual</i>
app: Cotizador Web	application-component	pkg: MiMutualWeb	<i>modulo: cotizador</i>
Aplicativo	application-function		<i>modulo: cotizador</i>
Compartido	application-function		<i>modulo: cotizador</i>
Cotizador	application-function		<i>modulo: cotizador</i>
Interfaz gráfica	application-function		<i>modulo: cotizador</i>
Util	application-function	En la Utilidades se especifican las clases que complementan una funcionalidad de un componente o servicio. * FormValidate: Clase que implementa un disparador de validación de todos los campos de un formulario. * CustomValidators: Creación de validaciones de campos.	<i>modulo: cotizador</i>
admin Páginas	application-function		<i>modulo: cotizador</i>
admin Servicios	application-function		<i>modulo: cotizador</i>
API Mi Mutual	application-interface		<i>modulo: mimutual</i>
Autenticación: authgard	application-service		
Interceptor: errorinterceptor	application-service		
Parametrización: typeservice	application-service		
Sesión admin: idletimeout	application-service		

ArqCotizador. 2. Contenedores

Mi Mutual. Coomeva, 2023.

Estructura de componentes principales, Cotizador Web, Mi Mutual. Roles de componentes, separación responsabilidades.

versión 0.2

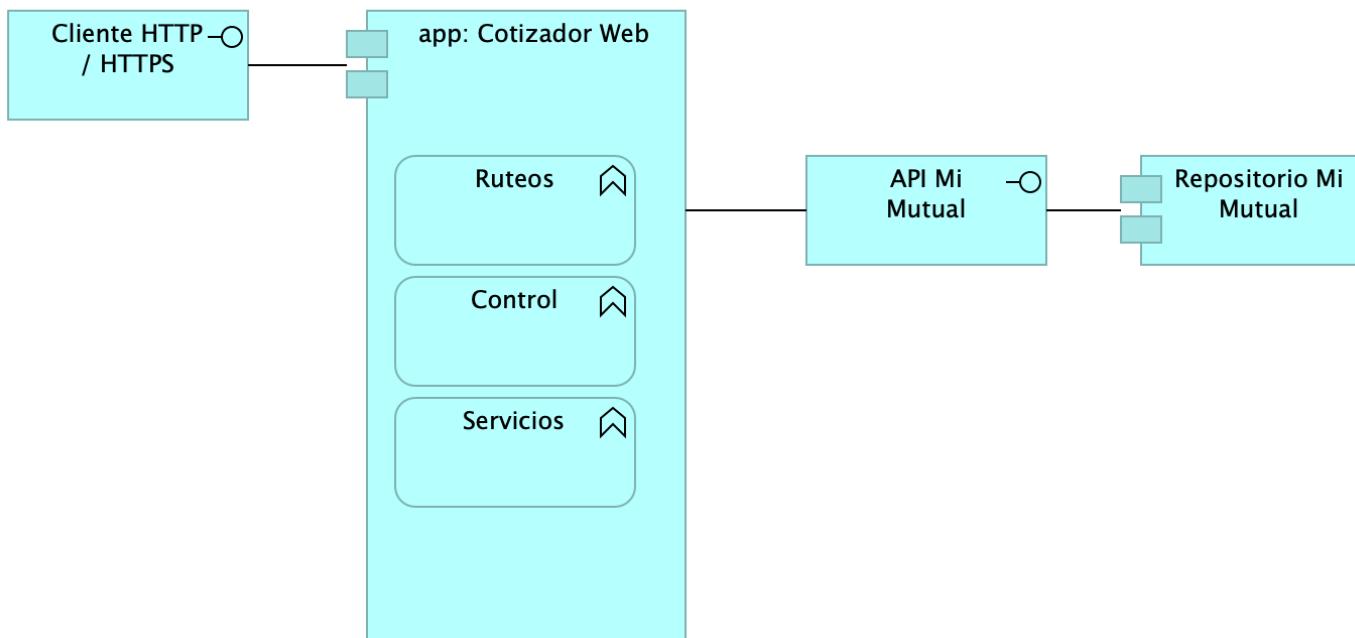


Imagen 60: Diagram: ArqCotizador. 2. Contenedores

Catálogo de Elementos

Name	Type	Description	Properties
Repositorio Mi Mutual	application-component	Antes SIPAS, Mi Mutual es una aplicación web compuesta por distintos módulos de software con arreglo a todas las actividades necesarias que soportan la operación de los productos y servicios que ofrece la Unidad de Solidaridad y Seguros de la Cooperativa. Para el manejo de la persistencia de datos se utilizará Spring Data el cual se apoya en la especificación de JPA y en la implementación de HIBERNATE además de complementar esta capa de persistencia con nuevas funcionalidades que facilitan el acceso a datos.	modulo: mimutual
app: Cotizador Web	application-component	pkg: MiMutualWeb	modulo: cotizador
Control	application-function		
Ruteos	application-function		
Servicios	application-function		
API Mi Mutual	application-interface		modulo: mimutual
Cliente HTTP / HTTPS	application-interface		

ArqCotizador. 4. Aplicación

Mi Mutual. Coomeva, 2023.
Organización de aplicación Cotizador Web, Mi Mutual. Estado Actual.
Segmentos (1) frontal, (2) servicios, (3) central/negocio Mi Mutual, (4) infraestructura.
versión 0.4.1

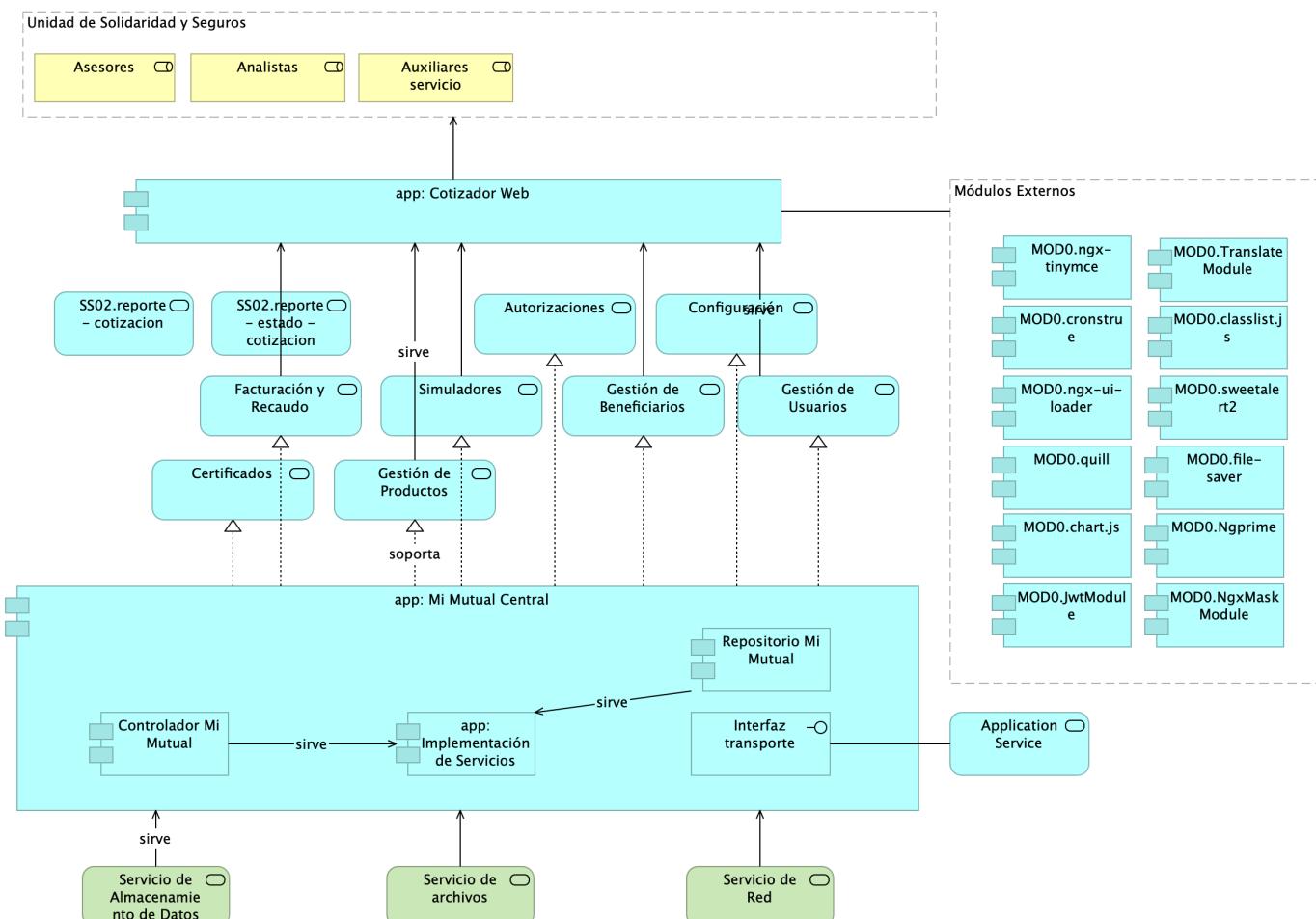


Imagen 61: Diagrama: ArqCotizador. 4. Aplicación

La organización de la aplicación Cotizador Web Mi Mutual, como capa de presentación y servicios, plantea una estructura basada en la referencia de aplicaciones Angular 12. Las características de esta estructura (referida por Angular) está orientada al crecimiento (tamaño) de la aplicación, la escalabilidad y al rendimiento. La aplicación web Cotizador está diseñada (modulos) para manejar la carga por demanda del contenido.

Catálogo de Elementos

Name	Type	Description	Properties
Controlador Mi Mutual	application-component	Los componentes de este tipo se encargan de controlar los servicios rest de la aplicación, además en estos componentes se define la forma como se reciben y envían los datos de los servicios rest y la seguridad de cada uno de los métodos.	<i>modulo: mimutual</i>
MODO.JwtModule	application-component	Manejo de token. Documentación: https://github.com/auth0/angular2-jwt	
MODO.Ngprime	application-component	Manejo de componentes visuales Documentación: https://www.primefaces.org/primeng/#/	
MODO.NgxMaskModule	application-component	Manejo de máscaras de input text. Documentación: https://github.com/JsDaddy/ngx-mask	
MODO.TranslateModule	application-component	Manejo de internacionalización. Documentación: https://github.com/ngx-translate/core	
MODO.chart.js	application-component	Componente utilizado para el manejo de gráficas Documentación: https://www.chartjs.org/docs/latest/	
MODO.classlist.js	application-component	Componete para el manejo de listas de datos en las gráficas Documentación: https://www.chartjs.org/docs/latest/	
MODO.crontrue	application-component	Componente para traducir una expresión cron a palabras Documentación: https://github.com/bradymholt/crontrue	
MODO.file-saver	application-component	Componente para descargar un archivo desde los bytes Documentación: https://github.com/eligrey/FileSaver.js#readme	
MODO.ngx-tinymce	application-component	Editor html para generación de plantillas para cartas Documentación: https://cipchk.github.io/ngx-tinymce/#/	
MODO.ngx-ui-loader	application-component	Manejo de Spinner para control de peticiones asíncronas. Documentación: https://github.com/t-ho/ngx-ui-loader	
MODO.quill	application-component	Ccomponente para editor html Documentación: https://quilljs.com/	
MODO/sweetalert2	application-component	Manejo de alertas de mensajes. Documentación: https://sweetalert2.github.io/	
Repositorio Mi Mutual	application-component	Antes SIPAS, Mi Mutual es una aplicación web compuesta por distintos módulos de software con arreglo a todas las actividades necesarias que soportan la operación de los productos y servicios que ofrece la Unidad de Solidaridad y Seguros de la Cooperativa. Para el manejo de la persistencia de datos se utilizará Spring Data el cual se apoya en la especificación de JPA y en la implementación de HIBERNATE además de complementar esta capa de persistencia con nuevas funcionalidades que facilitan el acceso a datos.	<i>modulo: mimutual</i>
app: Cotizador Web	application-component	pkg: MiMutualWeb	<i>modulo: cotizador</i>
app: Implementación de Servicios	application-component	Los componentes de este tipo se encargan de controlar y almacenar toda la lógica del negocio, validaciones y todo lo referente a procesamiento de datos.	<i>modulo: mimutual</i>
app: Mi Mutual Central	application-component	Antes SIPAS, Mi Mutual es una aplicación web compuesta por distintos módulos de software con arreglo a todas las actividades necesarias que soportan la operación de los productos y servicios que ofrece la Unidad de Solidaridad y Seguros de la Cooperativa.	<i>modulo: mimutual</i>
Interfaz transporte	application-interface	Feign Client. Integración con otros sistemas para facilitar los procesos de vinculación, retiro, reactivación o fallecimiento de asociados.	
Application Service	application-service	Otros servicios del contexto de Mi Mutual Central.	
Autorizaciones	application-service	Autorizaciones: Administración de peticiones de autorización y sus correspondientes aprobaciones usando el servicio del flujo de procesos.	

Name	Type	Description	Properties
Certificados	application-service	Certificados: Permite la generación de los certificados de valores de protección y contribuciones pagadas, de retención en la fuente, de pagos de perseverancia y de cobertura de auxilio funerario.	
Configuración	application-service	Configuración o parametrización de factores para realizar los cálculos de las contribuciones de los asociados a la Cooperativa para cada uno de los productos adquiridos.	
Facturación y Recaudo	application-service	Administración de la facturación y recaudo diario de los productos	
Gestión de Beneficiarios	application-service	Gestión de Beneficiarios: Permite administrar la información relacionada con los beneficiarios del Asociado, permitiendo ejecutar operaciones de consulta, inserción y modificación	
Gestión de Productos	application-service	Gestión de productos del fondo mutual y auxilio funerario que involucran lo relacionado a las siguientes coberturas: * Fondo de Solidaridad: Incapacidades temporales, Incapacidades Permanentes (total, parcial), Perseverancia 60, 62, 65, 70 años, Perseverancias Anticipadas, Fallecimiento Asociado (Auxilio por muerte), Desempleo, Disminución de ingresos y enfermedades graves; Rentas por hospitalización, Enfermedades de Alto Costo, Pólizas de seguros personales y patrimoniales, Planes educativos, Segunda opinión médica, Asistencias. * Auxilio Funerario: Fallecimiento de familiares directos (inscritos) del Asociado.	
Gestión de Usuarios	application-service	Gestión de Usuarios: Administración de la información relacionada con los usuarios del sistema. Este componente se comunica con el servicio unificado de autenticación y autorización que devuelve los permisos que un usuario posee sobre las opciones que proporciona el sistema.	
SS02.reporte - cotizacion	application-service		
SS02.reporte - estado - cotizacion	application-service		
Simuladores	application-service	Simuladores: Funcionalidades que permiten generar las simulaciones de los diferentes planes o modificaciones (incrementos y disminuciones) a los productos del Asociado.	
Analistas	business-role	Analistas y auxiliares de servicio regional y nacional, agentes del centro de contacto, auditores médicos, analistas de operaciones (aseguramiento y facturación) y jefes.	
Asesores	business-role	Asesores integrales	
Auxiliares servicio	business-role	Analistas y auxiliares de servicio regional y nacional, agentes del centro de contacto, auditores médicos, analistas de operaciones (aseguramiento y facturación) y jefes.	
Módulos Externos	grouping		
Unidad de Solidaridad y Seguros	grouping	La Unidad de Solidaridad y Seguros cuenta con un software integrado para su core de negocio denominado SIPAS (Sistema de Previsión, Asistencia y Solidaridad)	
Servicio de Almacenamiento de Datos	technology-service		
Servicio de Red	technology-service		
Servicio de archivos	technology-service		

ArqCotizador. 4a. Aplicación. Servicios

Mi Mutual. Coomeva, 2023.

Especificaciones de Servicios.
Aplicación Cotizador Web, Mi Mutual.
Estado Actual. Estructura interna,
comunicación e interfaces.

versión 0.1

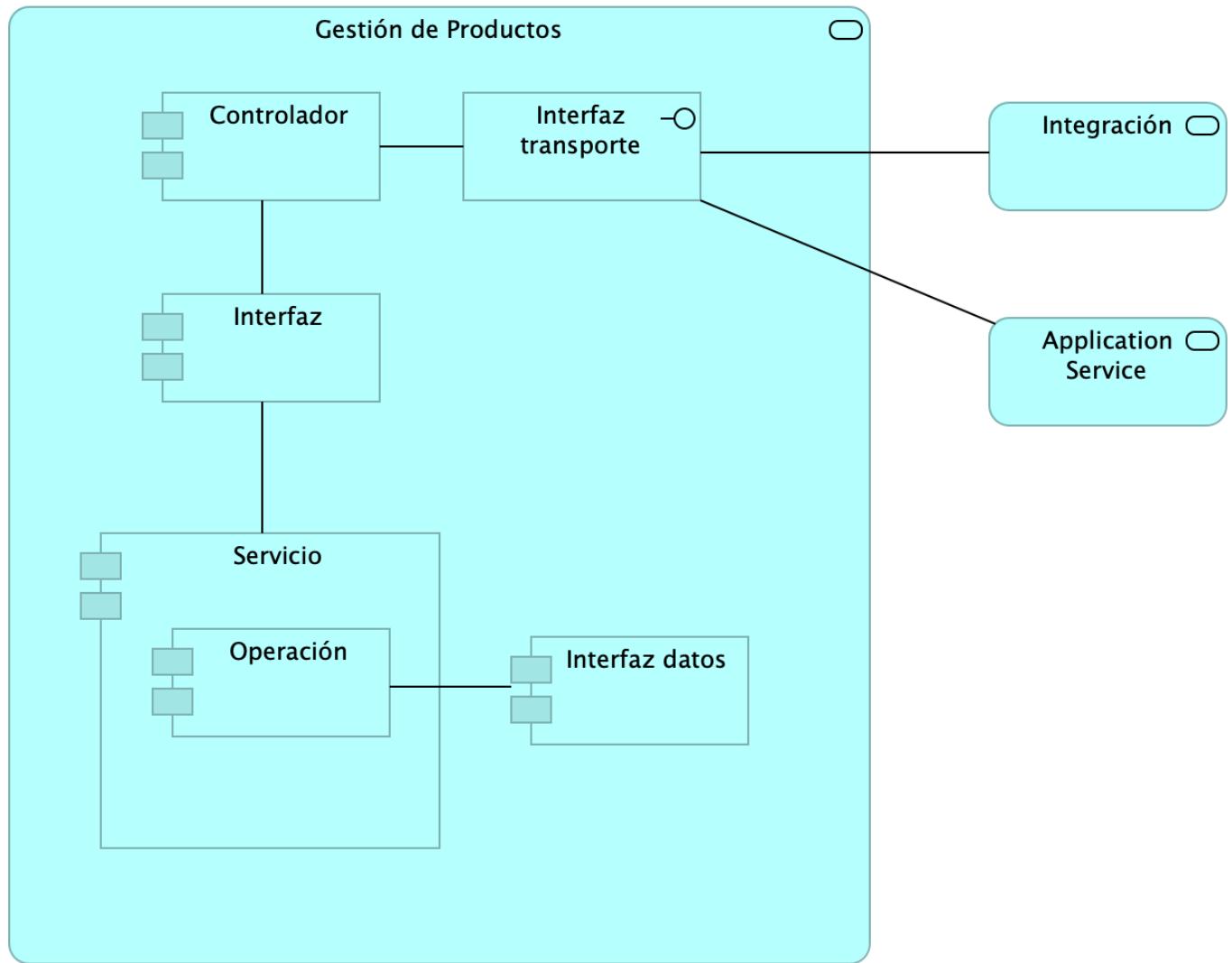


Imagen 62: Diagram: ArqCotizador. 4a. Aplicación. Servicios

Composición interna de los servicios de Mi Mutual Central, Mi Mutual Web, Cotizador Web.

Catálogo de Elementos

Name	Type	Description	Properties
Controlador	application-component	Controlador interno del servicio. Punto de entrada a la lógica de expuesta.	
Interfaz	application-component	Interfaz de inversión de dependencia a las clases del servicio.	
Interfaz datos	application-component	Acceso a datos del modelo del contexto de Mi Mutual Central.	
Operación	application-component		
Servicio	application-component	Exposición de componentes de negocio.	

Name	Type	Description	Properties
Interfaz transporte	application-interface	Feign Client. Integración con otros sistemas para facilitar los procesos de vinculación, retiro, reactivación o fallecimiento de asociados.	
Application Service	application-service	Otros servicios del contexto de Mi Mutual Central.	
Gestión de Productos	application-service	Gestión de productos del fondo mutual y auxilio funerario que involucran lo relacionado a las siguientes coberturas: * Fondo de Solidaridad: Incapacidades temporales, Incapacidades Permanentes (total, parcial), Perseverancia 60, 62, 65, 70 años, Perseverancias Anticipadas, Fallecimiento Asociado (Auxilio por muerte), Desempleo, Disminución de ingresos y enfermedades graves; Rentas por hospitalización, Enfermedades de Alto Costo, Pólizas de seguros personales y patrimoniales, Planes educativos, Segunda opinión médica, Asistencias. * Auxilio Funerario: Fallecimiento de familiares directos (inscritos) del Asociado.	
Integración	application-service		

ArqCotizador. 4a. Dependencias

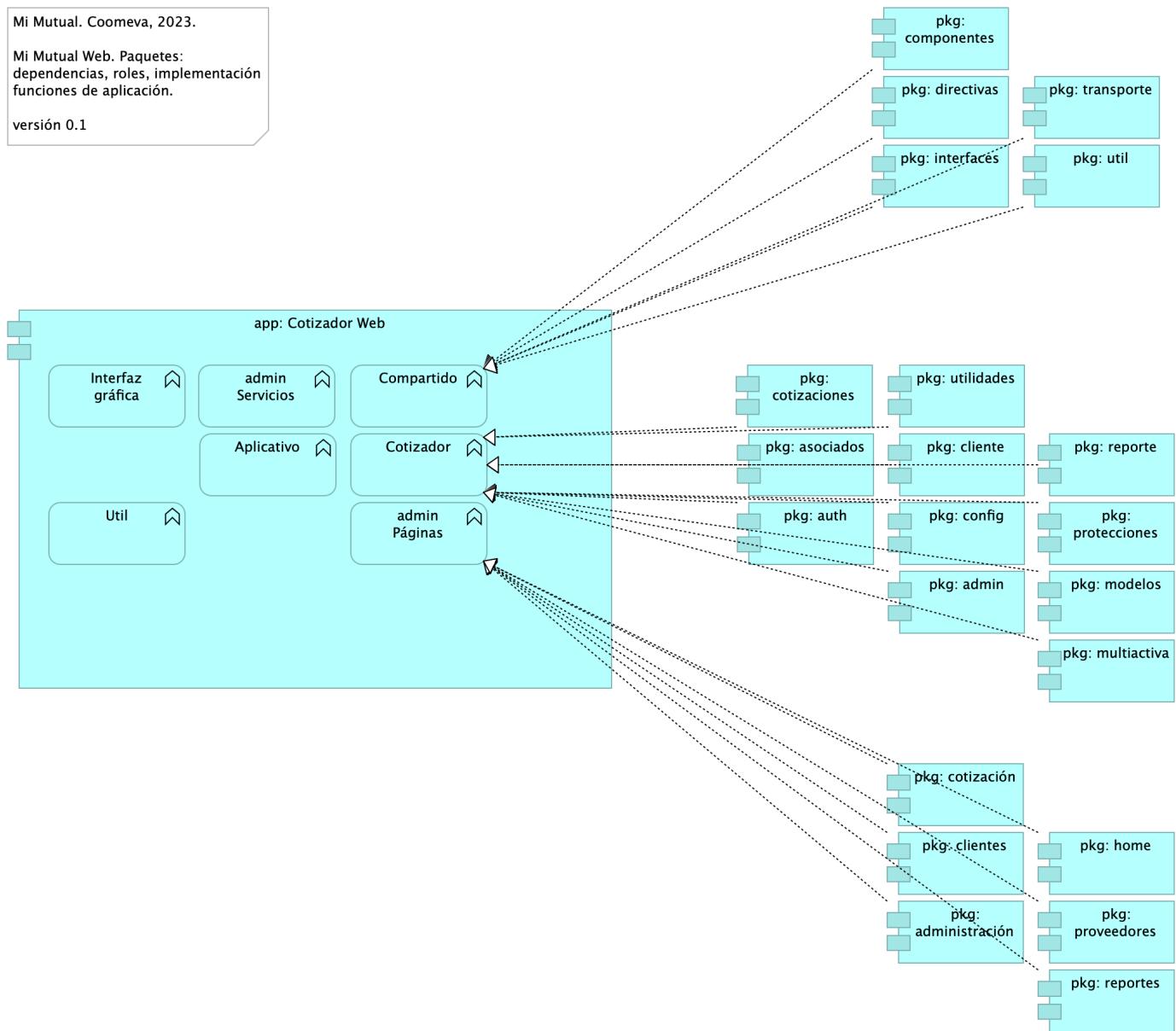


Imagen 63: Diagram: ArqCotizador. 4a. Dependencias

Paquetes y Dependencias Cotizador Web

Módulos y componentes que hacen parte de la estructura de la aplicación Cotizador Web (basado en Angular 12 [2](#)).

Módulos Cotizador Web

La estructura por módulos actual apunta a la escalabilidad y mantenimiento del Cotizador en términos de: organizar las partes de la aplicación, organización los bloques, extender la aplicación con librerías externas, proporcionar un entorno de resolución de plantillas y además, distribuir las cargas de los componentes y servicios que usa la aplicación.

Catálogo de Elementos

Name	Type	Description	Properties
app: Cotizador Web	application-component	pkg: MiMutualWeb	modulo: cotizador
pkg: admin	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	modulo: cotizador
pkg: administración	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	modulo: cotizador
pkg: asociados	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	modulo: cotizador
pkg: auth	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	modulo: cotizador
pkg: cliente	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	modulo: cotizador
pkg: clientes	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	modulo: cotizador
pkg: componentes	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	modulo: cotizador
pkg: config	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	modulo: cotizador
pkg: cotizaciones	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	modulo: cotizador
pkg: cotización	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	modulo: cotizador
pkg: directivas	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	modulo: cotizador
pkg: home	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	modulo: cotizador
pkg: interfaces	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	modulo: cotizador
pkg: modelos	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	modulo: cotizador
pkg: multiactiva	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	modulo: cotizador
pkg: protecciones	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	modulo: cotizador
pkg: proveedores	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	modulo: cotizador
pkg: reporte	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	modulo: cotizador
pkg: reportes	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	modulo: cotizador
pkg: transporte	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	modulo: cotizador
pkg: util	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	modulo: cotizador

Name	Type	Description	Properties
pkg: utilidades	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	<i>modulo: cotizador</i>
Aplicativo	application-function		<i>modulo: cotizador</i>
Compartido	application-function		<i>modulo: cotizador</i>
Cotizador	application-function		<i>modulo: cotizador</i>
Interfaz gráfica	application-function		<i>modulo: cotizador</i>
Util	application-function	En la Utilidades se especifican las clases que complementan una funcionalidad de un componente o servicio. * FormValidate: Clase que implementa un disparador de validación de todos los campos de un formulario. * CustomValidators: Creación de validaciones de campos.	<i>modulo: cotizador</i>
admin Páginas	application-function		<i>modulo: cotizador</i>
admin Servicios	application-function		<i>modulo: cotizador</i>

ArqCotizador. 5. Físico (despliegue)

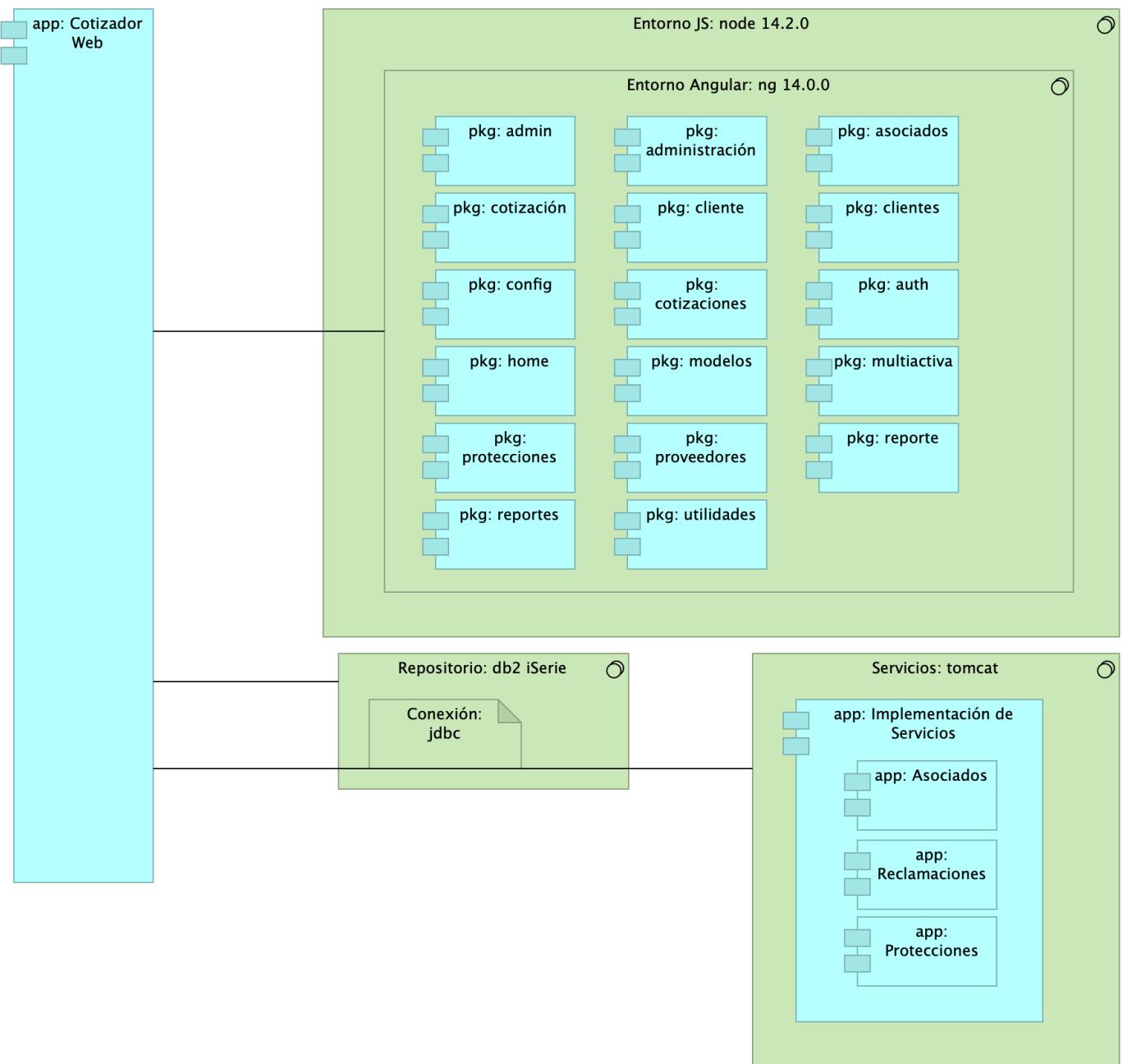


Imagen 64: Diagram: ArqCotizador. 5. Físico (despliegue)

Especificaciones de Despliegue Cotizador Web

Detalles de configuración del proyecto Mi Mutual en el espacio de trabajo local (2022).

Recursos Requeridos

- Git. Se debe instalar git para poder realizar la clonación de cada uno de los proyectos mas adelante.
- Instalación SmartGit. Se debe instalar Smartgit para poder realizar la clonación de cada uno de los proyectos mas adelante, este es opcional ya que es una interfaz gráfica de git mas amigable para el usuario en caso que no desee trabajar con la consola.
- DBeaver. Se debe instalar DBeaver para poder acceder a la base de datos.
- Instalación Maven. Se debe instalar maven para poder compilar los proyectos, nos debemos asegurar de instalar la versión 3.6.3, en caso que no se encuentra en la página oficial copiar la carpeta que esta en el repositorio a archivo de programas.
- Java 8. Se debe instalar Java para poder desplegar los proyectos mas adelante, nos debemos asegurar de instalar la versión 8.
- STS. Se debe instalar el IDE para realizar modificaciones a los proyectos back mas adelante en este caso Spring Tools 4 for Eclipse. La carpeta que genera el instalador la copiamos a archivos de programa.
- Instalación Lombok. Se debe instalar el lombok seleccionando el IDE que acabamos de instalar en este caso el STS.
- Postman. Se debe instalar el postman para poder consumir los servicios del backend mas adelante cuando ya se hayan desplegado.

- Node Js. Se debe instalar Node Js para configurar el proyecto front mas adelante, nos debemos asegurar de instalar la versión v14.2.0.
- Visual Studio Code. Se debe instalar el IDE para realizar modificaciones al proyecto front mas adelante en este caso Visual Studio code.
- Angular 14.

Catálogo de Elementos

Name	Type	Description	Properties
app: Asociados	application-component	Contiene todas las funcionalidades relacionadas con consulta y creación de asociados y beneficiarios.	<i>modulo: mimutual</i>
app: Cotizador Web	application-component	pkg: MiMutualWeb	<i>modulo: cotizador</i>
app: Implementación de Servicios	application-component	Los componentes de este tipo se encargan de controlar y almacenar toda la lógica del negocio, validaciones y todo lo referente a procesamiento de datos.	<i>modulo: mimutual</i>
app: Protecciones	application-component	Contiene todas las funcionalidades relacionadas con la gestión y configuración de productos y protecciones.	<i>modulo: mimutual</i>
app: Reclamaciones	application-component	Contiene todas las funcionalidades relacionadas con la gestión de reclamaciones, liquidaciones y pagos.	<i>modulo: mimutual</i>
pkg: admin	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	<i>modulo: cotizador</i>
pkg: administración	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	<i>modulo: cotizador</i>
pkg: asociados	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	<i>modulo: cotizador</i>
pkg: auth	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	<i>modulo: cotizador</i>
pkg: cliente	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	<i>modulo: cotizador</i>
pkg: clientes	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	<i>modulo: cotizador</i>
pkg: config	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	<i>modulo: cotizador</i>
pkg: cotizaciones	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	<i>modulo: cotizador</i>
pkg: cotización	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	<i>modulo: cotizador</i>
pkg: home	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	<i>modulo: cotizador</i>
pkg: modelos	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	<i>modulo: cotizador</i>
pkg: multiactiva	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	<i>modulo: cotizador</i>
pkg: protecciones	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	<i>modulo: cotizador</i>
pkg: proveedores	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	<i>modulo: cotizador</i>
pkg: reporte	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	<i>modulo: cotizador</i>
pkg: reportes	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	<i>modulo: cotizador</i>
pkg: utilidades	application-component	controller: Almacenan todas las clases que constituyen los servicios rest de la aplicación.	<i>modulo: cotizador</i>
Conexión: jdbc	artifact		<i>modulo: cotizador</i>
Entorno Angular: ng 14.0.0	system-software		<i>modulo: cotizador</i>

Name	Type	Description	Properties
Entorno JS: node 14.2.0	system-software		modulo: cotizador
Repositorio: db2 iSerie	system-software		modulo: cotizador
Servicios: tomcat	system-software		modulo: mimutual

ArqCotizador. 7. Datos. Negocio

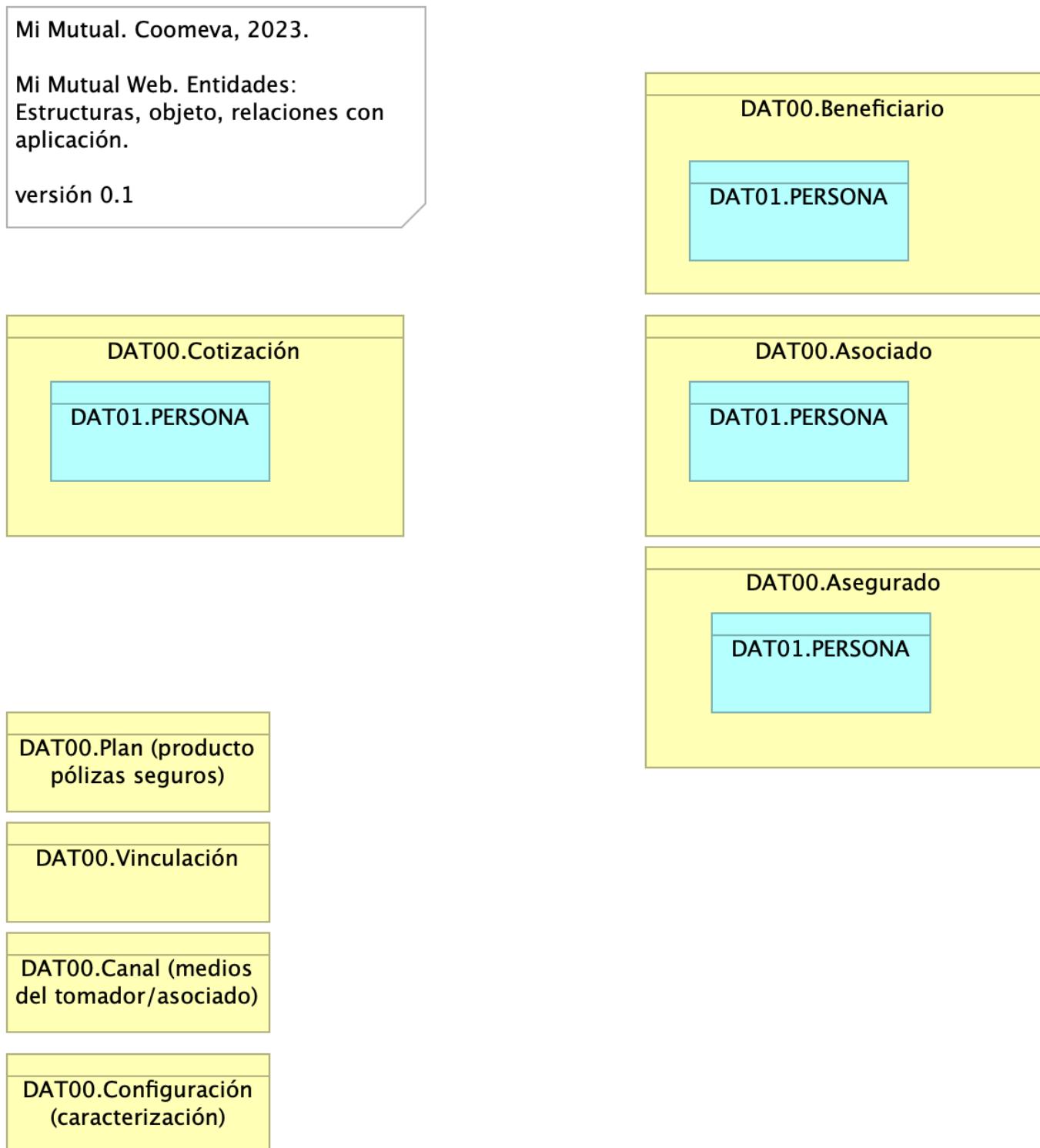


Imagen 65: Diagram: ArqCotizador. 7. Datos. Negocio

Entidades de Negocio Mi Mutual

Dominios de datos de negocio. Entidades independiente de la plataforma y de la tecnología.

- Configuración (caracterización de productos, plan)
- Plan (producto pólizas seguros)
- Canal (medios del tomador/asociado)

- Parámetros globales (catálogos)
- Portafolio de asociado
- Asociado
- Facturación
- Beneficiario

Catálogo de Elementos

Name	Type	Description	Properties
DAT00.Asegurado	business-object		
DAT00.Asoiado	business-object		
DAT00.Beneficiario	business-object		
DAT00.Canal (medios del tomador/asociado)	business-object		
DAT00.Configuración (caracterización)	business-object	Caracterización de productos, planes, parámetros	
DAT00.Cotización	business-object		
DAT00.Plan (producto pólizas seguros)	business-object		
DAT00.Vinculación	business-object		
DAT01.PERSONA	data-object		

Generated on: Wed Oct 25 2023 13:47:52 GMT-0500 (COT)

Requerimientos de Administración

1. Las soluciones deben permitir la administración de los Roles de Usuarios: esta funcionalidad debe permitir configurar los diferentes roles de los usuarios funcionales de los procesos.
2. Administrar los Perfiles de acceso por rol: Esta funcionalidad permitirá configurar a que funcionalidades u opciones de la solución puede entrar un usuario con un rol específico. Administrar los Usuarios de la Solución: Esta funcionalidad debe permitir configurar, activar, desactivar usuarios de las soluciones desarrolladas.
3. Administrar los permisos de acceso: Esta funcionalidad permite definir específicamente a que servicios de la solución puede ingresar un usuario (CRUD).
4. En los desarrollos se debe contar con un módulo de auditoría que permita generar consultas para conocer quién y cuándo se ha realizado una actuación determinada dentro de procesos críticos, almacenando el código del usuario la actuación, la acción, la fecha, la hora, y la dirección IP de la máquina.
5. Las soluciones deben permitir la configuración de permisos de consulta con diferentes alcances para cada tipo de usuario.
6. Desde la interfaz de usuario se debe poder crear, modificar o inactivar usuarios, perfiles o roles, permisos a las diferentes funcionalidades de la solución.
7. Las soluciones deben permitir la definición de varios tipos de usuario.
8. Las soluciones deben permitir la parametrización de los consecutivos que maneja la entidad para los diferentes documentos generados por las soluciones.
9. Debe permitir parametrizar la vinculación del consecutivo a un documento en forma manual o automática.
10. Las soluciones deben permitir que se configure la autenticación de forma interna integrándose con LDAP el acceso de los usuarios y actores de las diferentes dependencias de la entidad que interactúen con los demás sistemas.

Requerimientos de Seguridad

1. Las soluciones deben dar cumplimiento a las políticas institucionales del sistema de gestión de seguridad de la información establecidas por la entidad que busca garantizar la confidencialidad, integridad y disponibilidad de la información que se genera, procesa, almacena y/o transmite en los sistemas de Información de la Entidad.
2. Las soluciones de automatización de procesos a implementar deben permitir la Gestión de Seguridad de Usuarios, grupos de usuarios y asignación de Roles y perfiles de usuarios, permitiendo asociar las acciones disponibles en la solución con respecto a roles de usuario, permitiendo parametrizar las funcionalidades que cada actor puede usar en la solución.
3. Un usuario puede estar asociado a uno o más roles, de tal manera que los menús de navegación de la solución se muestran o despliegan dependiendo de las acciones asociadas a cada rol de usuario, permitiendo así que cuando el usuario es autenticado correctamente, la solución verifica los roles que tiene activos para otorgarle únicamente las acciones autorizadas.
4. El diseño de la solución debe definir los criterios necesarios para asegurar la trazabilidad y auditoría sobre las acciones de creación, actualización, modificación o borrado de los componentes de información, de tal manera que la solución debe permitirle al administrador de la solución parametrizar las tablas y eventos que pueden auditarse.
5. Las soluciones deben tener en cuenta mecanismos que aseguren el registro histórico para poder mantener la trazabilidad de las acciones realizadas por los usuarios, contemplando el registro de auditoría que contiene información de fecha y hora, identificación del registro, tabla afectada, descripción del evento, tipo de evento, usuario que realiza la acción, identificación de sesión y dirección IP del usuario que efectuó la transacción.
6. La solución debe proveer una consulta que permita a un usuario con los privilegios asignados, consultar los registros de auditoría, aplicando criterios de filtro (usuario, máquina, rango de fechas y tipo de operación).
7. Las soluciones deben integrarse con LDAP – (Lightweight Directory Access Protocol) para los procesos de inicio de sesión y autenticación. La solución debe soportar la integración Nativa con Active Directory de Microsoft. Para usuarios externos el mecanismo de autorización, autenticación y acceso será controlado a través del modelo de seguridad de la solución (no habrá autenticación para usuarios externos).

8. Las soluciones deben cumplir con los lineamientos de seguridad relacionados a su utilización a través de redes públicas y privadas, garantizando la confidencialidad e integridad de la información y acceso a ella.
9. Debe evidenciar que, a través de pruebas de vulnerabilidad, garantiza la seguridad de la información. Estas pruebas deben suministrar evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad.
10. Debe incluir un mecanismo de cifrado de los datos que se transportan entre los diferentes componentes tecnológicos y los datos sensibles de la base de datos que representen un alto nivel de confidencialidad.
11. A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio).
12. Debe contemplar el cumplimiento de la normatividad vigente en cuanto a protección de datos personales y debe permitir el manejo de excepciones.
13. Para los casos que aplique se debe permitir el manejo de certificados y/o firmas digitales en los documentos que así se definan para efectos de aprobación y digitalización.
14. Debe contemplar las prácticas de desarrollo seguro de aplicaciones y/o implementación segura de productos, para su naturaleza Web based.
15. Debe funcionar sobre protocolo SSL (certificados internos de la entidad cuando los sistemas de información sean internas y certificados validos públicamente cuando los sistemas de información estén expuestas a internet).
16. Debe entregar un procedimiento para el respaldo de la información de acuerdo con las necesidades de la entidad.
17. Debe incluir uso de criptografía para transacciones y/o campos sensibles según lo indiquen las normas vigentes y las necesidades específicas del negocio de acuerdo como lo determine la entidad.
18. Debe contemplar un modelo de datos que garantice base de datos única para evitar que se pueda presentar duplicidad de información.
19. En la información confidencial solo puede ser consultada por los perfiles autorizados e igualmente restringir documentos de consulta según los privilegios o permisos asociados.
20. A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio).
21. Debe cerrar las transacciones luego de máximo 10 minutos de inactividad.
22. Debe incluir controles de bloqueo de cuenta después de un máximo de 5 intentos erróneos a fin de evitar ataques de fuerza bruta.
23. Debe evidenciar el resultado positivo frente a pruebas de ethical hacking, análisis de vulnerabilidades, carga, estrés y desempeño antes de la puesta en operación de acuerdo con los lineamientos de la entidad.
24. Debe cumplir con todos los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la "Guía de desarrollo OWASP" y "OWAS Cheat Sheet".

Referencias

[1] [2] [3] [[eservices5-23?](#)] [[eservices6-12?](#)] [[eservices7-23?](#)] [[bptrends07?](#)]

1. **Stefanini. Proyecto de mejoramiento SIU de coomeva. Fase i**
Stefanini, Coomeva
(2022-06) <https://hwong23.github.io/fna-devdoc-f1/v/6497aef0f15c3591f0728e4c42cb2c26c13b43aa/>
2. **Procuraduría general de la nación. Anexo - especificaciones técnicas 19-05-2023**
Coomeva
(2023-05) <https://hwong23.github.io/fna-devdoc-f1/v/6497aef0f15c3591f0728e4c42cb2c26c13b43aa/>
3. **Coomeva manual técnico sharepoint, versión 1**
Stefanini, Coomeva
(2022-05) <https://hwong23.github.io/fna-devdoc-f1/v/6497aef0f15c3591f0728e4c42cb2c26c13b43aa/>

1. Angular 2 tiene una arquitectura Modelo Vista Controlador (MVC) con el fin de hacer el desarrollo gestionado.[←](#)

2. Angular 2 tiene una arquitectura Modelo Vista Controlador (MVC) con el fin de hacer el desarrollo gestionado.[←](#)