Documento de Arquitectura Migración Funcional PGN SIU

OP 078-2023 - Fase 2, PGN Migración Funcional SIU

**Versión** del producto 1.fa97e14 de 08 Nov 2023

**Presentado a**

Procuraduría General de la Nación (PGN)

**Fecha**

08 Nov 2023

Los productos de esta etapa, Migración Funcional SIU, Contrato 078-2023, ([Web](https://hwong23.github.io/pgn-078/v/fa97e143490a6cdd2c18ca213b366745be537235/)) están basados en el resultado de la Fase 1 del proyecto PGN SIU del 2022, [Sharepoint Softgic@fa97e14](http://softgic.sharepoint.com) del November 8, 2023.

## Autores

* **Harry Wong, ing.** · Usuario [e\_hwong](https://github.com/e_hwong) Arquitecto, Softgic

✉ — Enviar mensajes a Harry Wong, ing. <harry.wong@softgic.co>.

## Objetivo del Documento

Descripción de los productos del trabajo de arquitectura de la Fase 2, proyecto Migración Funcional SIU de la Procuraduría General de la Nación (PGN en adelante), Contrato 078-2023. 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, 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.

## Control de Cambios

| Tema | OP 078-2023 Fase 2, PGN Migración Funcional SIU |
| --- | --- |
| Palabras clave | SIU, Softgic, PGN, Análisis de brecha, GAP, Comparativa |
| Autor |  |
| Fuente |  |
| **Versión** |  |
| 1.fa97e14 | 2023-11-08. arqdoc2 |
| 1.c296a03 | 2023-11-07. Merge branch ‘main’ of https://github.com/hwong23/pgn-078 |
| 1.57a9a5e | 2023-11-07. arqdoc |
| 1.bc63c34 | 2023-10-27. ing–indcdr |
| 1.c61d86d | 2023-10-27. riesgos2 |
| 1.bd83343 | 2023-10-27. riesgos |
| 1.3a67565 | 2023-10-22. output readme–version |
| 1.15ac385 | 2023-10-22. histr27 |
| 1.a97248b | 2023-10-22. histr26 |
| 1.ef11c3e | 2023-10-22. histr25 |
| Vínculos | [N003a Vista Segmento PGN SIU](N03a%a20Vsta%20aSegenta%20SOA%20PGN.md) |

## Contenidos

Table of Contents

# Introducción

## Propósito

Este documento tiene como propósito presentar la arquitectura del aplicativo Sistema Único de Información (SUI) para Procuraduría General de la Nación (PGN). 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 como tal. Este documento puede ser 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

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

Lista de restricciones de la migración SUI, 2023.

1. Restricciones de hardware o software en servidores. Los equipos de infraestructura del proyecto actual a tener en cuenta en los diseños de la solución de esta Fase 2 serán los mismos de la anterior Fase 1. Esto es, los que están descritos en el anexo técnico del contrato del proyecto.
2. Disponibilidad de recursos. Los recursos de implementación y validación de calidad de esta Fase del proyecto son los mismos a tener en cuenta en los diseños de la solución de esta Fase 2. Otros recursos a considerar son los descritos en el anexo técnico del contrato del proyecto.
3. Estándares. Los estándares seleccionados por la solución de este proyecto, (Fase 2, PGN Migración Funcional SIU, están determinados por el uso de las plataformas específicas determinadas por la implementación (desarrollo del software).
4. Requerimientos de interoperabilidad. Los recursos de interoperabilidad y colaboración entre sistemas, módulos, submódulos y aplicaciones de terceros relacionados con esta Fase del proyecto son los mismos a tener en cuenta en los diseños de la solución de esta Fase 2. Otros recursos a considerar son los descritos en el anexo técnico del contrato del proyecto.
5. Requerimientos de protocolos o interfaces. Los recursos de red, y protocolos de comunicación o transporte de esta Fase del proyecto a tener en cuenta en los diseños de la solución de esta Fase 2 parten de la base de los considerados en la anterior Fase 1. Otros recursos a considerar son los descritos en el anexo técnico del contrato del proyecto.
6. Seguridad. Las restricciones de seguridad del proyecto actual a tener en cuenta en los diseños de la solución de esta Fase 2 parten de la base de las de la anterior Fase 1. Esto es, los que están descritos en el anexo técnico del contrato del proyecto.

## 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 migración SUI, objeto de este proyecto, OP 078-2023.

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 SUI 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 SUI (lógica)

Tabla 1: Requisito no. 1, Migración SUI, Consistencia.

| Requisito | Extensibilidad SUI |
| --- | --- |
| Descripción | 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 sistémica | La consistencia persigue que el resultado de la lógica de negocio sea la misma entre los módulos del SUI 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 SUI

Tabla 2: Requisito no. 2, Mantenibilidad SUI.

| Requisito | Mantenibilidad SUI |
| --- | --- |
| Descripción | Evitar las dependencia transitivas de los módulos misionales del SUI a componentes y sistemas de terceros o submódulos no misionales. |
| Calidad sistémica | 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. |

### Extensibilidad SUI

Tabla 3: Requisito no. 3, Migración SUI, Flexibilidad.

| 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. |

# Documento de Arquitectura del SIU Migración Funcional

* [Patrón de Diseño Línea Base SUI PGN](#patrón-de-diseño-línea-base-sui-pgn)
  + [Lineabase.0.SIU applicación](#lineabase.0.siu-applicación)
  + [Lineabase.1.SIU componente](#lineabase.1.siu-componente)
  + [Lineabase.1a.SIU componentes. infraestrcutura](#X72fb0e13deea73ab81b6017cb7efce1fdaee8fb)
  + [Linebase.2.Portal](#linebase.2.portal)
* [Patrón de Diseño Migración SUI PGN](#patrón-de-diseño-migración-sui-pgn)
  + [Migracion.1a.a.SIU Contexto Módulo](#migracion.1a.a.siu-contexto-módulo)
  + [Migracion.1b.1. SIU Módulos Componentes](#migracion.1b.1.-siu-módulos-componentes)
  + [Migracion.1c.SIU Modulos Colaboración](#migracion.1c.siu-modulos-colaboración)
  + [Migracion.1b.1. SIU Módulos Componentes](#migracion.1b.1.-siu-módulos-componentes)
  + [Migracion.1b.2. SIU Módulos Componentes. Brecha](#X94ce159eae10be57afd13515fdf00a0751e6438)
  + [Migracion.1b.3. SIU Módulos Clases](#migracion.1b.3.-siu-módulos-clases)
  + [Migracion.2d2. Datos. Organización](#migracion.2d2.-datos.-organización)
  + [Migracion.2d3. Datos. Transporte (flujo SUI - SIM)](#Xfbf704b660659b6e8d0d346e8d16af3e8ac0b46)
  + [Migracion.2d4. Datos. Transporte (flujo SUI - SUI)](#Xabd414ca24770512cc2268d2b3818bdd39c63da)
  + [Migracion.6. Migración de datos](#migracion.6.-migración-de-datos)
* [Organización Cambios Arquitectura](#organización-cambios-arquitectura)
  + [Organización. 1n. Mapa producto](#organización.-1n.-mapa-producto)
  + [Organización. 1n.1.b. Mapa producto PGN. Relatoría](#X41d75eeb32073b8941fb782816a746d44007ab9)
  + [Organización. 2n.1a. Mapa producto PGN. Conciliacion](#X77eeae52cdb9a163e5d64ec38732a647f5ed87b)
  + [Organización. 4n.1. Mapa producto PGN. Estratego](#X7fb2109b67dc1249864a78b191ce4b8a389267d)
  + [Organización. 3n.1. Mapa producto PGN. SIAF](#X1930f7df0bd023582609abce4634c2ec8c945c8)
* [Arquitectura de Seguridad, SUI Migración](#arquitectura-de-seguridad,-sui-migración)
  + [Seguridad.1. Requerimientos](#seguridad.1.-requerimientos)
  + [Seguridad. Linebase.2.Portal](#seguridad.-linebase.2.portal)
* [Análisis de Productos](#análisis-de-productos)
  + [Organización. 4n.1a. Mapa producto PGN. Comparativa](#Xb0beaf2f037d17a4a34f272b378a0d10c97537f)
* [Riesgos Técnicos](#riesgos-técnicos)
  + [Riesgos.1. Migración funcional](#riesgos.1.-migración-funcional)
  + [Riesgos.2. Modelo Riesgo RSG10](#riesgos.2.-modelo-riesgo-rsg10)

# Patrón de Diseño Línea Base SUI PGN

## Lineabase.0.SIU applicación



Imagen 1: Diagram: Lineabase.0.SIU applicación

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

### Catálogo de Elementos

| Name | Type | Description | Properties |
| --- | --- | --- | --- |
| **Application Collaboration** | application-collaboration |  |  |
| **Application Collaboration** | application-collaboration |  |  |
| **App** | application-component |  | *plataforma:* node Js*brecha:* 100 |
| **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 analisis 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 obliaciones legales y éticas con respecto a la perdida de informacion confidencial por parte de ciudadanos del pais. La informacion 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 2013La metodologia empleada tendrá las siguientes fases: • FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como:o Recopilación de dominios/IPs/puertos/servicioso Recopilación de metadatoso Uso de Google Dorks.• ANÁLSIS 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 códigoo Inclusión de ficheros locales o remotoso Evasión de autenticacióno Carencia de controles de autorizacióno Ejecución de comandos en el lado del servidoro Ataques tipo Cross Site Request Forgeryo Control de erroreso Gestión de sesioneso Fugas de informacióno Secuestros de sesióno 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 adiciones con el objetivo de comprobar la criticidad de esta.No URL IP1. https://runtimetest.lappiz.io/#/auth/login/PGN\_Lappiz135.181.185.207 | *plantilla:* element-md-bold*brecha:* 100 |
| **App PGN Web** | application-component | Los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la “Guía de desarrollo OWASP” y “OWAS Cheat Sheet, permitirá realizar pruebas de seguridad integrando el analisis de vulnerabilidades, y pruebas de Ethical Hacking. Los resultados permitirán identificar los requisitos de seguridad que los sistemas de informacion o servicios web deberán cumplir.La metodologia empleada tendrá las siguientes fases: • FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como:o Recopilación de dominios/IPs/puertos/servicioso Recopilación de metadatoso Uso de Google Dorks.• ANÁLSIS 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 códigoo Inclusión de ficheros locales o remotoso Evasión de autenticacióno Carencia de controles de autorizacióno Ejecución de comandos en el lado del servidoro Ataques tipo Cross Site Request Forgeryo Control de erroreso Gestión de sesioneso Fugas de informacióno Secuestros de sesióno 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 adiciones con el objetivo de comprobar la criticidad de esta.No URL IP1. https://runtimetest.lappiz.io/#/auth/login/PGN\_Lappiz135.181.185.207El 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. | *plataforma:* angular 11*brecha:* 100 |
| **Config** | application-component |  | *plataforma:* cs |
| **Punto acceso público** | application-interface | URL tipo CHTTP |  |
| **Application Service (NLB)** | application-service |  | *plataforma:* angular 11*brecha:* 100 |
| **Interfaz de datos 1** | application-service |  |  |
| **Interfaz de datos 2** | application-service |  |  |

## Lineabase.1.SIU componente



Imagen 2: Diagram: 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

### Catálogo de Elementos

| Name | Type | Description | Properties |
| --- | --- | --- | --- |
| **Persistencia** | application-collaboration |  |  |
| **App** | application-component |  | *plataforma:* node Js*brecha:* 100 |
| **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 analisis 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 obliaciones legales y éticas con respecto a la perdida de informacion confidencial por parte de ciudadanos del pais. La informacion 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 2013La metodologia empleada tendrá las siguientes fases: • FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como:o Recopilación de dominios/IPs/puertos/servicioso Recopilación de metadatoso Uso de Google Dorks.• ANÁLSIS 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 códigoo Inclusión de ficheros locales o remotoso Evasión de autenticacióno Carencia de controles de autorizacióno Ejecución de comandos en el lado del servidoro Ataques tipo Cross Site Request Forgeryo Control de erroreso Gestión de sesioneso Fugas de informacióno Secuestros de sesióno 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 adiciones con el objetivo de comprobar la criticidad de esta.No URL IP1. https://runtimetest.lappiz.io/#/auth/login/PGN\_Lappiz135.181.185.207 | *plantilla:* element-md-bold*brecha:* 100 |
| **App PGN Web** | application-component | Los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la “Guía de desarrollo OWASP” y “OWAS Cheat Sheet, permitirá realizar pruebas de seguridad integrando el analisis de vulnerabilidades, y pruebas de Ethical Hacking. Los resultados permitirán identificar los requisitos de seguridad que los sistemas de informacion o servicios web deberán cumplir.La metodologia empleada tendrá las siguientes fases: • FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como:o Recopilación de dominios/IPs/puertos/servicioso Recopilación de metadatoso Uso de Google Dorks.• ANÁLSIS 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 códigoo Inclusión de ficheros locales o remotoso Evasión de autenticacióno Carencia de controles de autorizacióno Ejecución de comandos en el lado del servidoro Ataques tipo Cross Site Request Forgeryo Control de erroreso Gestión de sesioneso Fugas de informacióno Secuestros de sesióno 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 adiciones con el objetivo de comprobar la criticidad de esta.No URL IP1. https://runtimetest.lappiz.io/#/auth/login/PGN\_Lappiz135.181.185.207El 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. | *plataforma:* angular 11*brecha:* 100 |
| **Config** | application-component |  | *plataforma:* cs |
| **Controlador admin** | application-component |  | *plataforma:* cs |
| **Controlador frontal mvl** | application-component |  | *plataforma:* js |
| **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. | *plataforma:* js |
| **Controlador funcional** | application-component |  | *plataforma:* js |
| **Modelo (neg)** | application-component |  | *plataforma:* cs |
| **Puerto datos 1** | application-component |  | *plataforma:* js |
| **Puerto datos 2** | application-component |  | *plataforma:* cs |
| **Seguridad** | application-component |  | *plataforma:* sql*brecha:* 100 |
| **Transacciones** | application-component |  | *plataforma:* sql*brecha:* 100 |
| **Utilitario** | application-component |  | *plataforma:* no-sql |
| **Vista móvil** | application-component |  | *plataforma:* js |
| **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.NETHuellas 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” | *plataforma:* html |
| **Interfaz de aplicación (runtime)** | application-interface | Servidor web: Microsoft-IIS/10.0 Marco de Programación: ASP.NETHuellas 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” | *plataforma:* angular 11 |
| **API externas** | application-service |  |  |
| **Application Service (NLB)** | application-service |  | *plataforma:* angular 11*brecha:* 100 |
| **Archivos Compartidos** | application-service |  |  |
| **CDN Contenidos** | application-service |  | *brecha:* 100 |
| **Doku (gest. doc.)** | application-service |  | *brecha:* 100 |
| **Identidades** | application-service |  |  |
| **Interfaz de datos 1** | application-service |  |  |
| **Interfaz de datos 2** | application-service |  |  |
| **Interfaz de datos 3** | application-service |  |  |
| **ccccc Proveedores contenidos** | application-service |  | *brecha:* 100 |
| **Mensaje: JSON** | data-object |  |  |
| **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 conclifcto entre ellos.El api transaccional construida en Node js con ORM Sequelize cuenta con obligatoriedad de token tipo bearer generado desde Api config (Api security token generado con autenticación de directorio activo o login de usuario externo) cuenta con un modelo de capas donde primero se encuentra un DTO consistente en estructura de datos y métodos de “check permissions” (un endpoint del api de seguridad para validar privilegios sobre las acciones de la petición en ingreso) luego dependiendo del tipo de transacción se tiene una capa para Lappiz functions, Lappiz Jobs (Tareas programables) y Lappiz model (Generado con base ORM sequelize). Todas las transacciones una vez son validadas en token y permisos, pasan a un tenedor de conexión para modificar las cadenas de conexión en marcha y saber que usuario de bd va a efectuar la operación y con qué privilegios. Todas las peticiones entran en un modelo natural de node js compuesto por un Event queue y un evento Loop; estas peticiones se procesan en la base de datos y todas las excepciones controladas se registran en un log de errores en formato txt con las especificaciones y devolviendo errores controlados con protocolos HTTPs al Runtime (front de SUI). |  |
| **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. |  |

## Lineabase.1a.SIU componentes. infraestrcutura



Imagen 3: Diagram: Lineabase.1a.SIU componentes. infraestrcutura

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)

### Catálogo de Elementos

| Name | Type | Description | Properties |
| --- | --- | --- | --- |
| **Persistencia** | application-collaboration |  |  |
| **App** | application-component |  | *plataforma:* node Js*brecha:* 100 |
| **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 analisis 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 obliaciones legales y éticas con respecto a la perdida de informacion confidencial por parte de ciudadanos del pais. La informacion 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 2013La metodologia empleada tendrá las siguientes fases: • FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como:o Recopilación de dominios/IPs/puertos/servicioso Recopilación de metadatoso Uso de Google Dorks.• ANÁLSIS 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 códigoo Inclusión de ficheros locales o remotoso Evasión de autenticacióno Carencia de controles de autorizacióno Ejecución de comandos en el lado del servidoro Ataques tipo Cross Site Request Forgeryo Control de erroreso Gestión de sesioneso Fugas de informacióno Secuestros de sesióno 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 adiciones con el objetivo de comprobar la criticidad de esta.No URL IP1. https://runtimetest.lappiz.io/#/auth/login/PGN\_Lappiz135.181.185.207 | *plantilla:* element-md-bold*brecha:* 100 |
| **App PGN Web** | application-component | Los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la “Guía de desarrollo OWASP” y “OWAS Cheat Sheet, permitirá realizar pruebas de seguridad integrando el analisis de vulnerabilidades, y pruebas de Ethical Hacking. Los resultados permitirán identificar los requisitos de seguridad que los sistemas de informacion o servicios web deberán cumplir.La metodologia empleada tendrá las siguientes fases: • FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como:o Recopilación de dominios/IPs/puertos/servicioso Recopilación de metadatoso Uso de Google Dorks.• ANÁLSIS 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 códigoo Inclusión de ficheros locales o remotoso Evasión de autenticacióno Carencia de controles de autorizacióno Ejecución de comandos en el lado del servidoro Ataques tipo Cross Site Request Forgeryo Control de erroreso Gestión de sesioneso Fugas de informacióno Secuestros de sesióno 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 adiciones con el objetivo de comprobar la criticidad de esta.No URL IP1. https://runtimetest.lappiz.io/#/auth/login/PGN\_Lappiz135.181.185.207El 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. | *plataforma:* angular 11*brecha:* 100 |
| **Config** | application-component |  | *plataforma:* cs |
| **Controlador admin** | application-component |  | *plataforma:* cs |
| **Controlador frontal mvl** | application-component |  | *plataforma:* js |
| **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. | *plataforma:* js |
| **Controlador funcional** | application-component |  | *plataforma:* js |
| **Modelo (neg)** | application-component |  | *plataforma:* cs |
| **Puerto datos 1** | application-component |  | *plataforma:* js |
| **Puerto datos 2** | application-component |  | *plataforma:* cs |
| **Seguridad** | application-component |  | *plataforma:* sql*brecha:* 100 |
| **Transacciones** | application-component |  | *plataforma:* sql*brecha:* 100 |
| **Utilitario** | application-component |  | *plataforma:* no-sql |
| **Vista móvil** | application-component |  | *plataforma:* js |
| **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.NETHuellas 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” | *plataforma:* html |
| **Interfaz de aplicación (runtime)** | application-interface | Servidor web: Microsoft-IIS/10.0 Marco de Programación: ASP.NETHuellas 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” | *plataforma:* angular 11 |
| **API externas** | application-service |  |  |
| **Application Service (NLB)** | application-service |  | *plataforma:* angular 11*brecha:* 100 |
| **Archivos Compartidos** | application-service |  |  |
| **CDN Contenidos** | application-service |  | *brecha:* 100 |
| **Doku (gest. doc.)** | application-service |  | *brecha:* 100 |
| **Identidades** | application-service |  |  |
| **Interfaz de datos 1** | application-service |  |  |
| **Interfaz de datos 2** | application-service |  |  |
| **Interfaz de datos 3** | application-service |  |  |
| **ccccc Proveedores contenidos** | application-service |  | *brecha:* 100 |
| **Mensaje: JSON** | data-object |  |  |
| **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. |  |
| **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 conclifcto entre ellos.El api transaccional construida en Node js con ORM Sequelize cuenta con obligatoriedad de token tipo bearer generado desde Api config (Api security token generado con autenticación de directorio activo o login de usuario externo) cuenta con un modelo de capas donde primero se encuentra un DTO consistente en estructura de datos y métodos de “check permissions” (un endpoint del api de seguridad para validar privilegios sobre las acciones de la petición en ingreso) luego dependiendo del tipo de transacción se tiene una capa para Lappiz functions, Lappiz Jobs (Tareas programables) y Lappiz model (Generado con base ORM sequelize). Todas las transacciones una vez son validadas en token y permisos, pasan a un tenedor de conexión para modificar las cadenas de conexión en marcha y saber que usuario de bd va a efectuar la operación y con qué privilegios. Todas las peticiones entran en un modelo natural de node js compuesto por un Event queue y un evento Loop; estas peticiones se procesan en la base de datos y todas las excepciones controladas se registran en un log de errores en formato txt con las especificaciones y devolviendo errores controlados con protocolos HTTPs al Runtime (front de SUI). |  |
| **Servidor BDD App** | node | Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 GhzDiscos 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 GhzDiscos 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. |  |

## Linebase.2.Portal



Imagen 4: Diagram: 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

### Catálogo de Elementos

| Name | Type | Description | Properties |
| --- | --- | --- | --- |
| **Application Collaboration Sharepoint** | application-collaboration |  |  |
| **Servidor aplicaciones Sharepoint** | application-component |  |  |
| **Servidor datos Sharepoint** | application-component |  |  |
| **Servidor web Sharepoint** | application-component |  |  |
| **Application Interface** | application-interface |  |  |

# Patrón de Diseño Migración SUI PGN

## Migracion.1a.a.SIU Contexto Módulo



Imagen 5: Diagram: Migracion.1a.a.SIU Contexto Módulo

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 dell 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).

### Catálogo de Elementos

| Name | Type | Description | Properties |
| --- | --- | --- | --- |
| **cc:Administración** | application-collaboration |  |  |
| **cc:Almacenamiento** | application-collaboration | Espacio de almancenamiento 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 partigular 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 |  |  |
| **interfaz** | application-interface |  |  |
| **interfaz** | application-interface |  |  |
| **interfaz** | application-interface |  |  |
| **interfaz** | application-interface |  |  |
| **Cliente PGN** | business-actor |  |  |
| **Funcionario PGN** | business-actor |  |  |
| **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 sistémica: la consistencia persigue que el resultado de la lógica de negocio sea la misma entre los módulos del SUI 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. |  |
| **ARQ02. Mantenibilidad SUI** | constraint | Evitar las dependencia transitivas de los módulos misionales del SUI a componentes y sistemas de terceros o submódulos no misionales. Calidad sistémica: 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 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. |  |
| **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. |  |
| **RQR. Seguridad** | requirement | Requerimientos de seguridad, SUI, Migración, en aspectos de comunicación, autenticación, autorización y (manejo de) sesiones. |  |

## Migracion.1b.1. SIU Módulos Componentes



Imagen 6: Diagram: Migracion.1b.1. SIU Módulos Componentes

Presentación de los componentes internos de los submódulos del sistema único de información migrado, SUI de PGN. Organización intena de los servicios y paquetes que integran cada submódulo del SUI. Todos los sistemas de información del SUI siguen esta directiva: estarán constituídos 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 tecnologeias. 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.

### Catálogo de Elementos

| Name | Type | Description | Properties |
| --- | --- | --- | --- |
| **cc:PGN SUI (módulo central)** | application-collaboration | Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular 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. |  |
| **App** | application-component |  | *plataforma:* node Js*brecha:* 100 |
| **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 analisis 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 obliaciones legales y éticas con respecto a la perdida de informacion confidencial por parte de ciudadanos del pais. La informacion 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 2013La metodologia empleada tendrá las siguientes fases: • FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como:o Recopilación de dominios/IPs/puertos/servicioso Recopilación de metadatoso Uso de Google Dorks.• ANÁLSIS 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 códigoo Inclusión de ficheros locales o remotoso Evasión de autenticacióno Carencia de controles de autorizacióno Ejecución de comandos en el lado del servidoro Ataques tipo Cross Site Request Forgeryo Control de erroreso Gestión de sesioneso Fugas de informacióno Secuestros de sesióno 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 adiciones con el objetivo de comprobar la criticidad de esta.No URL IP1. https://runtimetest.lappiz.io/#/auth/login/PGN\_Lappiz135.181.185.207 | *plantilla:* element-md-bold*brecha:* 100 |
| **App PGN Web** | application-component | Los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la “Guía de desarrollo OWASP” y “OWAS Cheat Sheet, permitirá realizar pruebas de seguridad integrando el analisis de vulnerabilidades, y pruebas de Ethical Hacking. Los resultados permitirán identificar los requisitos de seguridad que los sistemas de informacion o servicios web deberán cumplir.La metodologia empleada tendrá las siguientes fases: • FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como:o Recopilación de dominios/IPs/puertos/servicioso Recopilación de metadatoso Uso de Google Dorks.• ANÁLSIS 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 códigoo Inclusión de ficheros locales o remotoso Evasión de autenticacióno Carencia de controles de autorizacióno Ejecución de comandos en el lado del servidoro Ataques tipo Cross Site Request Forgeryo Control de erroreso Gestión de sesioneso Fugas de informacióno Secuestros de sesióno 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 adiciones con el objetivo de comprobar la criticidad de esta.No URL IP1. https://runtimetest.lappiz.io/#/auth/login/PGN\_Lappiz135.181.185.207El 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. | *plataforma:* angular 11*brecha:* 100 |
| **CU ejecutable** | application-component |  | *plataforma:* js |
| **CU ejecutable (n)** | application-component |  | *plataforma:* js |
| **Config** | application-component |  | *plataforma:* cs |
| **Controlador admin** | application-component |  | *plataforma:* cs |
| **Controlador frontal mvl** | application-component |  | *plataforma:* js |
| **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. | *plataforma:* js |
| **Controlador funcional** | application-component |  | *plataforma:* js |
| **Función PGN 1** | application-component | La unidad de cómputo que resulta en la aplicación de una regla de negocio. | *plataforma:* js |
| **Modelo (neg)** | application-component |  | *plataforma:* cs |
| **Puerto datos 1** | application-component |  | *plataforma:* js |
| **Puerto datos 2** | application-component |  | *plataforma:* cs |
| **Seguridad** | application-component |  | *plataforma:* sql*brecha:* 100 |
| **Servidor aplicaciones Sharepoint** | application-component |  |  |
| **Servidor datos Sharepoint** | application-component |  |  |
| **Servidor web Sharepoint** | application-component |  |  |
| **Transacciones** | application-component |  | *plataforma:* sql*brecha:* 100 |
| **Utilitario** | application-component |  | *plataforma:* no-sql |
| **Vista móvil** | application-component |  | *plataforma:* js |
| **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.NETHuellas 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” | *plataforma:* html |
| **Application Interface** | application-interface |  |  |
| **Interfaz de aplicación (runtime)** | application-interface | Servidor web: Microsoft-IIS/10.0 Marco de Programación: ASP.NETHuellas 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” | *plataforma:* angular 11 |
| **API externas** | application-service |  |  |
| **Application Service (NLB)** | application-service |  | *plataforma:* angular 11*brecha:* 100 |
| **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 |  | *brecha:* 100 |
| **Doku (gest. doc.)** | application-service |  | *brecha:* 100 |
| **Identidades** | application-service |  |  |
| **Interfaz de datos 1** | application-service |  |  |
| **Interfaz de datos 2** | application-service |  |  |
| **Interfaz de datos 3** | application-service |  |  |
| **Office** | application-service |  |  |
| **ccccc Proveedores contenidos** | application-service |  | *brecha:* 100 |
| **Entidad negocio PGN 1** | business-object | Repreesnta un objeto de negocio del contexto de la entidad PGN,, por ejemplo: un decreto, una intervención, una conciliación. |  |
| **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 sistémica: la consistencia persigue que el resultado de la lógica de negocio sea la misma entre los módulos del SUI 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. |  |
| **ARQ02. Mantenibilidad SUI** | constraint | Evitar las dependencia transitivas de los módulos misionales del SUI a componentes y sistemas de terceros o submódulos no misionales. Calidad sistémica: 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 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. |  |
| **Mensaje: JSON** | data-object |  |  |
| **Administración** | grouping |  |  |
| **Almacenamiento** | grouping |  |  |
| **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. |  |
| **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. |  |
| **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. |  |
| **RQR. Seguridad** | requirement | Requerimientos de seguridad, SUI, Migración, en aspectos de comunicación, autenticación, autorización y (manejo de) sesiones. |  |

## Migracion.1c.SIU Modulos Colaboración



Imagen 7: Diagram: Migracion.1c.SIU Modulos Colaboración

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 estadar 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 comunición mediante mesajería, datos, ni

### Catálogo de Elementos

| Name | Type | Description | Properties |
| --- | --- | --- | --- |
| **cc:Almacenamiento** | application-collaboration | Espacio de almancenamiento 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 partigular de la PGN. |  |
| **cc:PGN SUI (módulo central)** | application-collaboration | Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular de la PGN. |  |
| **cc:PGN SUI (módulo central) 2** | application-collaboration | Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular 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. |  |
| **App** | application-component |  | *plataforma:* node Js*brecha:* 100 |
| **API SUI** | application-interface | API de representación del módulo. Centrlalización de la comunicación con otros módulos del SUI migrado. |  |
| **API SUI** | application-interface | API de representación del módulo. Centrlalización de la comunicación con otros módulos del SUI migrado. |  |
| **API SUI 2** | application-interface | API de representación del módulo. Centrlalización de la comunicación con otros módulos del SUI migrado. |  |

## Migracion.1b.1. SIU Módulos Componentes



Imagen 8: Diagram: Migracion.1b.1. SIU Módulos Componentes

Presentación de los componentes internos de los submódulos del sistema único de información migrado, SUI de PGN. Organización intena de los servicios y paquetes que integran cada submódulo del SUI. Todos los sistemas de información del SUI siguen esta directiva: estarán constituídos 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 tecnologeias. 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.

### Catálogo de Elementos

| Name | Type | Description | Properties |
| --- | --- | --- | --- |
| **cc:PGN SUI (módulo central)** | application-collaboration | Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular 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. |  |
| **App** | application-component |  | *plataforma:* node Js*brecha:* 100 |
| **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 analisis 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 obliaciones legales y éticas con respecto a la perdida de informacion confidencial por parte de ciudadanos del pais. La informacion 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 2013La metodologia empleada tendrá las siguientes fases: • FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como:o Recopilación de dominios/IPs/puertos/servicioso Recopilación de metadatoso Uso de Google Dorks.• ANÁLSIS 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 códigoo Inclusión de ficheros locales o remotoso Evasión de autenticacióno Carencia de controles de autorizacióno Ejecución de comandos en el lado del servidoro Ataques tipo Cross Site Request Forgeryo Control de erroreso Gestión de sesioneso Fugas de informacióno Secuestros de sesióno 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 adiciones con el objetivo de comprobar la criticidad de esta.No URL IP1. https://runtimetest.lappiz.io/#/auth/login/PGN\_Lappiz135.181.185.207 | *plantilla:* element-md-bold*brecha:* 100 |
| **App PGN Web** | application-component | Los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la “Guía de desarrollo OWASP” y “OWAS Cheat Sheet, permitirá realizar pruebas de seguridad integrando el analisis de vulnerabilidades, y pruebas de Ethical Hacking. Los resultados permitirán identificar los requisitos de seguridad que los sistemas de informacion o servicios web deberán cumplir.La metodologia empleada tendrá las siguientes fases: • FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como:o Recopilación de dominios/IPs/puertos/servicioso Recopilación de metadatoso Uso de Google Dorks.• ANÁLSIS 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 códigoo Inclusión de ficheros locales o remotoso Evasión de autenticacióno Carencia de controles de autorizacióno Ejecución de comandos en el lado del servidoro Ataques tipo Cross Site Request Forgeryo Control de erroreso Gestión de sesioneso Fugas de informacióno Secuestros de sesióno 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 adiciones con el objetivo de comprobar la criticidad de esta.No URL IP1. https://runtimetest.lappiz.io/#/auth/login/PGN\_Lappiz135.181.185.207El 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. | *plataforma:* angular 11*brecha:* 100 |
| **CU ejecutable** | application-component |  | *plataforma:* js |
| **CU ejecutable (n)** | application-component |  | *plataforma:* js |
| **Config** | application-component |  | *plataforma:* cs |
| **Controlador admin** | application-component |  | *plataforma:* cs |
| **Controlador frontal mvl** | application-component |  | *plataforma:* js |
| **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. | *plataforma:* js |
| **Controlador funcional** | application-component |  | *plataforma:* js |
| **Función PGN 1** | application-component | La unidad de cómputo que resulta en la aplicación de una regla de negocio. | *plataforma:* js |
| **Modelo (neg)** | application-component |  | *plataforma:* cs |
| **Puerto datos 1** | application-component |  | *plataforma:* js |
| **Puerto datos 2** | application-component |  | *plataforma:* cs |
| **Seguridad** | application-component |  | *plataforma:* sql*brecha:* 100 |
| **Servidor aplicaciones Sharepoint** | application-component |  |  |
| **Servidor datos Sharepoint** | application-component |  |  |
| **Servidor web Sharepoint** | application-component |  |  |
| **Transacciones** | application-component |  | *plataforma:* sql*brecha:* 100 |
| **Utilitario** | application-component |  | *plataforma:* no-sql |
| **Vista móvil** | application-component |  | *plataforma:* js |
| **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.NETHuellas 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” | *plataforma:* html |
| **Application Interface** | application-interface |  |  |
| **Interfaz de aplicación (runtime)** | application-interface | Servidor web: Microsoft-IIS/10.0 Marco de Programación: ASP.NETHuellas 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” | *plataforma:* angular 11 |
| **API externas** | application-service |  |  |
| **Application Service (NLB)** | application-service |  | *plataforma:* angular 11*brecha:* 100 |
| **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 |  | *brecha:* 100 |
| **Doku (gest. doc.)** | application-service |  | *brecha:* 100 |
| **Identidades** | application-service |  |  |
| **Interfaz de datos 1** | application-service |  |  |
| **Interfaz de datos 2** | application-service |  |  |
| **Interfaz de datos 3** | application-service |  |  |
| **Office** | application-service |  |  |
| **ccccc Proveedores contenidos** | application-service |  | *brecha:* 100 |
| **Entidad negocio PGN 1** | business-object | Repreesnta un objeto de negocio del contexto de la entidad PGN,, por ejemplo: un decreto, una intervención, una conciliación. |  |
| **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 sistémica: la consistencia persigue que el resultado de la lógica de negocio sea la misma entre los módulos del SUI 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. |  |
| **ARQ02. Mantenibilidad SUI** | constraint | Evitar las dependencia transitivas de los módulos misionales del SUI a componentes y sistemas de terceros o submódulos no misionales. Calidad sistémica: 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 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. |  |
| **Mensaje: JSON** | data-object |  |  |
| **Administración** | grouping |  |  |
| **Almacenamiento** | grouping |  |  |
| **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. |  |
| **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. |  |
| **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. |  |
| **RQR. Seguridad** | requirement | Requerimientos de seguridad, SUI, Migración, en aspectos de comunicación, autenticación, autorización y (manejo de) sesiones. |  |

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



Imagen 9: Diagram: Migracion.1b.2. SIU Módulos Componentes. Brecha

Los elementos resaltados indican las extensiones a la arqutecutra 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 construído 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 constituídos por submódulos dispuestos en relación de utilitarios (que sirven) a los componentes misionales del SUI, ubicados en el centro en la diagrama.

### Catálogo de Elementos

| Name | Type | Description | Properties |
| --- | --- | --- | --- |
| **App** | application-component |  | *plataforma:* node Js*brecha:* 100 |
| **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 analisis 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 obliaciones legales y éticas con respecto a la perdida de informacion confidencial por parte de ciudadanos del pais. La informacion 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 2013La metodologia empleada tendrá las siguientes fases: • FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como:o Recopilación de dominios/IPs/puertos/servicioso Recopilación de metadatoso Uso de Google Dorks.• ANÁLSIS 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 códigoo Inclusión de ficheros locales o remotoso Evasión de autenticacióno Carencia de controles de autorizacióno Ejecución de comandos en el lado del servidoro Ataques tipo Cross Site Request Forgeryo Control de erroreso Gestión de sesioneso Fugas de informacióno Secuestros de sesióno 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 adiciones con el objetivo de comprobar la criticidad de esta.No URL IP1. https://runtimetest.lappiz.io/#/auth/login/PGN\_Lappiz135.181.185.207 | *plantilla:* element-md-bold*brecha:* 100 |
| **App PGN Web** | application-component | Los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la “Guía de desarrollo OWASP” y “OWAS Cheat Sheet, permitirá realizar pruebas de seguridad integrando el analisis de vulnerabilidades, y pruebas de Ethical Hacking. Los resultados permitirán identificar los requisitos de seguridad que los sistemas de informacion o servicios web deberán cumplir.La metodologia empleada tendrá las siguientes fases: • FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como:o Recopilación de dominios/IPs/puertos/servicioso Recopilación de metadatoso Uso de Google Dorks.• ANÁLSIS 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 códigoo Inclusión de ficheros locales o remotoso Evasión de autenticacióno Carencia de controles de autorizacióno Ejecución de comandos en el lado del servidoro Ataques tipo Cross Site Request Forgeryo Control de erroreso Gestión de sesioneso Fugas de informacióno Secuestros de sesióno 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 adiciones con el objetivo de comprobar la criticidad de esta.No URL IP1. https://runtimetest.lappiz.io/#/auth/login/PGN\_Lappiz135.181.185.207El 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. | *plataforma:* angular 11*brecha:* 100 |
| **CU ejecutable** | application-component |  | *plataforma:* js |
| **CU ejecutable (n)** | application-component |  | *plataforma:* js |
| **Config** | application-component |  | *plataforma:* cs |
| **Controlador admin** | application-component |  | *plataforma:* cs |
| **Controlador frontal mvl** | application-component |  | *plataforma:* js |
| **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. | *plataforma:* js |
| **Controlador funcional** | application-component |  | *plataforma:* js |
| **Función PGN 1** | application-component | La unidad de cómputo que resulta en la aplicación de una regla de negocio. | *plataforma:* js |
| **Modelo (neg)** | application-component |  | *plataforma:* cs |
| **Puerto datos 1** | application-component |  | *plataforma:* js |
| **Puerto datos 2** | application-component |  | *plataforma:* cs |
| **Seguridad** | application-component |  | *plataforma:* sql*brecha:* 100 |
| **Servidor aplicaciones Sharepoint** | application-component |  |  |
| **Servidor datos Sharepoint** | application-component |  |  |
| **Servidor web Sharepoint** | application-component |  |  |
| **Transacciones** | application-component |  | *plataforma:* sql*brecha:* 100 |
| **Utilitario** | application-component |  | *plataforma:* no-sql |
| **Vista móvil** | application-component |  | *plataforma:* js |
| **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.NETHuellas 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” | *plataforma:* html |
| **Application Interface** | application-interface |  |  |
| **Interfaz de aplicación (runtime)** | application-interface | Servidor web: Microsoft-IIS/10.0 Marco de Programación: ASP.NETHuellas 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” | *plataforma:* angular 11 |
| **API externas** | application-service |  |  |
| **Application Service (NLB)** | application-service |  | *plataforma:* angular 11*brecha:* 100 |
| **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 |  | *brecha:* 100 |
| **Doku (gest. doc.)** | application-service |  | *brecha:* 100 |
| **Identidades** | application-service |  |  |
| **Interfaz de datos 1** | application-service |  |  |
| **Interfaz de datos 2** | application-service |  |  |
| **Interfaz de datos 3** | application-service |  |  |
| **Office** | application-service |  |  |
| **ccccc Proveedores contenidos** | application-service |  | *brecha:* 100 |
| **Entidad negocio PGN 1** | business-object | Repreesnta un objeto de negocio del contexto de la entidad PGN,, por ejemplo: un decreto, una intervención, una conciliación. |  |
| **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 sistémica: la consistencia persigue que el resultado de la lógica de negocio sea la misma entre los módulos del SUI 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. |  |
| **ARQ02. Mantenibilidad SUI** | constraint | Evitar las dependencia transitivas de los módulos misionales del SUI a componentes y sistemas de terceros o submódulos no misionales. Calidad sistémica: 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 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. |  |
| **Mensaje: JSON** | data-object |  |  |
| **Administración** | grouping |  |  |
| **Almacenamiento** | grouping |  |  |
| **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 conclifcto entre ellos.El api transaccional construida en Node js con ORM Sequelize cuenta con obligatoriedad de token tipo bearer generado desde Api config (Api security token generado con autenticación de directorio activo o login de usuario externo) cuenta con un modelo de capas donde primero se encuentra un DTO consistente en estructura de datos y métodos de “check permissions” (un endpoint del api de seguridad para validar privilegios sobre las acciones de la petición en ingreso) luego dependiendo del tipo de transacción se tiene una capa para Lappiz functions, Lappiz Jobs (Tareas programables) y Lappiz model (Generado con base ORM sequelize). Todas las transacciones una vez son validadas en token y permisos, pasan a un tenedor de conexión para modificar las cadenas de conexión en marcha y saber que usuario de bd va a efectuar la operación y con qué privilegios. Todas las peticiones entran en un modelo natural de node js compuesto por un Event queue y un evento Loop; estas peticiones se procesan en la base de datos y todas las excepciones controladas se registran en un log de errores en formato txt con las especificaciones y devolviendo errores controlados con protocolos HTTPs al Runtime (front de SUI). |  |
| **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. |  |
| **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. |  |
| **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. |  |
| **RQR. Seguridad** | requirement | Requerimientos de seguridad, SUI, Migración, en aspectos de comunicación, autenticación, autorización y (manejo de) sesiones. |  |

## Migracion.1b.3. SIU Módulos Clases



Imagen 10: Diagram: Migracion.1b.3. SIU Módulos Clases

El modelo de negocio del SIU Migrado sigue el patrón de diseño descrito en esta vista.

El diseño actual antepone un servicio como punto de entrada a un caso de uso, de tal forma que este se encarga únicamente (por resposabilidad) de coordinar las entradas y las salidas del caso de uso.

El modelo propicia la separación de la lógica de aplicación y la lógica de negocio. En este diseño, la primera está encapsulada en el Caso de Uso ejecutable (en el diagrama), mientras que la lógica de negocio lo está en una función de negocio.

Los conceptos de negocio están representados por funciones PGN (en el diagrama). Ejemplo: en el dominio de una conciliación, Función PGN 1 puede representar una nueva radicación en cumplimiento de las reglas de ese dominio. Esta función de negocio es completamente independiente del modelo de datos subyacente. Nótese que las entidades de datos de negocio no son accesibles desde la función de negocio.

### Catálogo de Elementos

| Name | Type | Description | Properties |
| --- | --- | --- | --- |
| **cc:PGN SUI (módulo central)** | application-collaboration | Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular de la PGN. |  |
| **CU ejecutable** | application-component |  | *plataforma:* js |
| **Función PGN 1** | application-component | La unidad de cómputo que resulta en la aplicación de una regla de negocio. | *plataforma:* js |
| **Función PGN 2** | application-component | La unidad de cómputo que resulta en la aplicación de una regla de negocio. | *plataforma:* js |
| **Modelo entrada** | application-component |  |  |
| **Modelo salida** | application-component |  |  |
| **Entrada** | application-function |  |  |
| **Estado** | application-function |  |  |
| **Función negocio** | application-function |  |  |
| **Reglas negocio** | application-function |  |  |
| **Resultado** | application-function |  |  |
| **Retorno** | application-function |  |  |
| **Validación entrada** | application-function |  |  |
| **Validación negocio** | application-function |  |  |
| **Verificación / consistencia** | application-function |  |  |
| **CU <>** | application-interface |  |  |
| **Persistencia <>** | application-interface |  |  |
| **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. |  |
| **Entidad negocio PGN 1** | business-object | Repreesnta un objeto de negocio del contexto de la entidad PGN,, por ejemplo: un decreto, una intervención, una conciliación. |  |

## Migracion.2d2. Datos. Organización



Imagen 11: Diagram: Migracion.2d2. Datos. Organización

Modelo de acceso y procesamiento a datos de negocio del SUI. La imagen siguiente presenta la organización de los ítems de transporte de datos de negocio necesarios para que los módulos del SUI puedan recolectar, procesar, integrar y almacenarlo de forma organizada y escalable.

Mediante esta organización, los datos de negocio son transportados desde sus respectivas fuentes mediante interfaces (principio de extensión y mantenibilidad referidos en las restricciones de la arquitecura del SUI Migrado). Los datos externos, entendidos como los de otros proveedores, son obtenidos mediante un intermediario: una API externa (*reverse proxy*).

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

### Catálogo de Elementos

| Name | Type | Description | Properties |
| --- | --- | --- | --- |
| **cc:PGN SUI (módulo central)** | application-collaboration | Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular de la PGN. |  |
| **cc:PGN SUI (módulo central) 2** | application-collaboration | Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular de la PGN. |  |
| **APP1.Relatoría** | application-component | Módulo del SUI. Relatoría pública. Publicación de información de referencia para funcionarios y personas naturales, cientes de la PGN. |  |
| **APP2.SIRI** | application-component | Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular de la PGN: SIRI. |  |
| **APP3.Control interno** | application-component | Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular de la PGN: Control Interno. |  |
| **APP4.Hominis** | application-component | Módulo del SUI. Gestión de capital humano, funcionarios y cargos de representación y libre remoción de la PGN. |  |
| **APP6.Estratego** | application-component | Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular de la PGN: Estratego. |  |
| **Interacción SUI - SIM** | application-interaction | Interacción de API SUI con API SIM para el transporte de entidades de negocio. Los tipos de datos que utilizan esta interacción entre aplicaciones son los datos externos al módulo central SUI que los requiera, los datos históricos que están por fuera del móduo SUI migrado, y los datos transaccionales de otros módulos SUI migrados. |  |
| **Interfaz de Acceso Proveedores** | application-interface | Interfaz de acceso a los tipos de datos externos al SUI.El patrón de API Externa (reverse proxie) tiene el rol de unir y referir a los datos externos e históricos al SIU Migrado de tal manera que hace transparente la localización y el formato de este tipo de datos. |  |
| **Interfaz de Almacenaniento** | application-interface | Interfaz de acceso a los repositorio, base de datos relacionales y no jerárquicas. Tipos de datos transaccionales, internos, del SUI. |  |
| **Procesamiento de lotes PGN** | application-process | Los procesos de lotes, que requieren volumenes de datos altos, deben hacer parte de la arquitectura de datos del SUI. |  |
| **API Externa (flujo de datos)** | application-service | El patrón de API Externa (reverse proxie) tiene el rol de unir y referir a los datos externos e históricos al SIU Migrado 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 SUI** | data-object |  |  |
| **Datos transaccionales módulo SUI** | data-object | Registros de trabajo de un módulo SUI Migrado, 2023. |  |

## Migracion.2d3. Datos. Transporte (flujo SUI - SIM)



Imagen 12: Diagram: Migracion.2d3. Datos. Transporte (flujo SUI - SIM)

Modelo de acceso a datos de negocio del SIM.

La imagen siguiente presenta la organización de los ítems de transporte de datos de negocio necesarios para que los módulos del SUI puedan recolectar, procesar, integrar y almacenarlo de forma organizada y escalable.

Mediante esta organización, los datos de negocio son transportados desde sus respectivas fuentes mediante interfaces (principio de extensión y mantenibilidad referidos en las restricciones de la arquitecura del SUI Migrado). Los datos externos, entendidos como los de otros proveedores, son obtenidos mediante un intermediario: una API externa (*reverse proxy*).

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

### Catálogo de Elementos

| Name | Type | Description | Properties |
| --- | --- | --- | --- |
| **cc:PGN SUI (módulo central)** | application-collaboration | Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular de la PGN. |  |
| **APP5.SIM** | application-component | Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular de la PGN: SIM. |  |
| **Interacción SUI - SIM** | application-interaction | Interacción de API SUI con API SIM para el transporte de entidades de negocio. Los tipos de datos que utilizan esta interacción entre aplicaciones son los datos externos al módulo central SUI que los requiera, los datos históricos que están por fuera del móduo SUI migrado, y los datos transaccionales de otros módulos SUI migrados. |  |
| **Interfaz de Acceso Proveedores** | application-interface | Interfaz de acceso a los tipos de datos externos al SUI.El patrón de API Externa (reverse proxie) tiene el rol de unir y referir a los datos externos e históricos al SIU Migrado de tal manera que hace transparente la localización y el formato de este tipo de datos. |  |
| **Interfaz de Almacenaniento** | application-interface | Interfaz de acceso a los repositorio, base de datos relacionales y no jerárquicas. Tipos de datos transaccionales, internos, del SUI. |  |
| **Datos externos** | data-object |  |  |
| **Datos históricos** | data-object |  |  |
| **Datos transaccionales módulo SUI** | data-object | Registros de trabajo de un módulo SUI Migrado, 2023. |  |

## Migracion.2d4. Datos. Transporte (flujo SUI - SUI)



Imagen 13: Diagram: Migracion.2d4. Datos. Transporte (flujo SUI - SUI)

Modelo de acceso y procesamiento a datos de negocio del SUI. La imagen siguiente presenta la organización de los ítems de transporte de datos de negocio necesarios para que los módulos del SUI puedan recolectar, procesar, integrar y almacenarlo de forma organizada y escalable.

Mediante esta organización, los datos de negocio son transportados desde sus respectivas fuentes mediante interfaces (principio de extensión y mantenibilidad referidos en las restricciones de la arquitecura del SUI Migrado). Los datos externos, entendidos como los de otros proveedores, son obtenidos mediante un intermediario: una API externa (*reverse proxy*).

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

### Catálogo de Elementos

| Name | Type | Description | Properties |
| --- | --- | --- | --- |
| **cc:PGN SUI (módulo central)** | application-collaboration | Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular de la PGN. |  |
| **cc:PGN SUI (módulo central) 2** | application-collaboration | Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular de la PGN. |  |
| **Interfaz de Acceso Proveedores** | application-interface | Interfaz de acceso a los tipos de datos externos al SUI.El patrón de API Externa (reverse proxie) tiene el rol de unir y referir a los datos externos e históricos al SIU Migrado de tal manera que hace transparente la localización y el formato de este tipo de datos. |  |
| **Interfaz de Acceso Proveedores 2** | application-interface | Interfaz de acceso a los tipos de datos externos al SUI.El patrón de API Externa (reverse proxie) tiene el rol de unir y referir a los datos externos e históricos al SIU Migrado de tal manera que hace transparente la localización y el formato de este tipo de datos. |  |
| **Interfaz de Almacenaniento** | application-interface | Interfaz de acceso a los repositorio, base de datos relacionales y no jerárquicas. Tipos de datos transaccionales, internos, del SUI. |  |
| **Datos transaccionales SUI** | data-object |  |  |
| **Datos transaccionales módulo SUI** | data-object | Registros de trabajo de un módulo SUI Migrado, 2023. |  |

## Migracion.6. Migración de datos

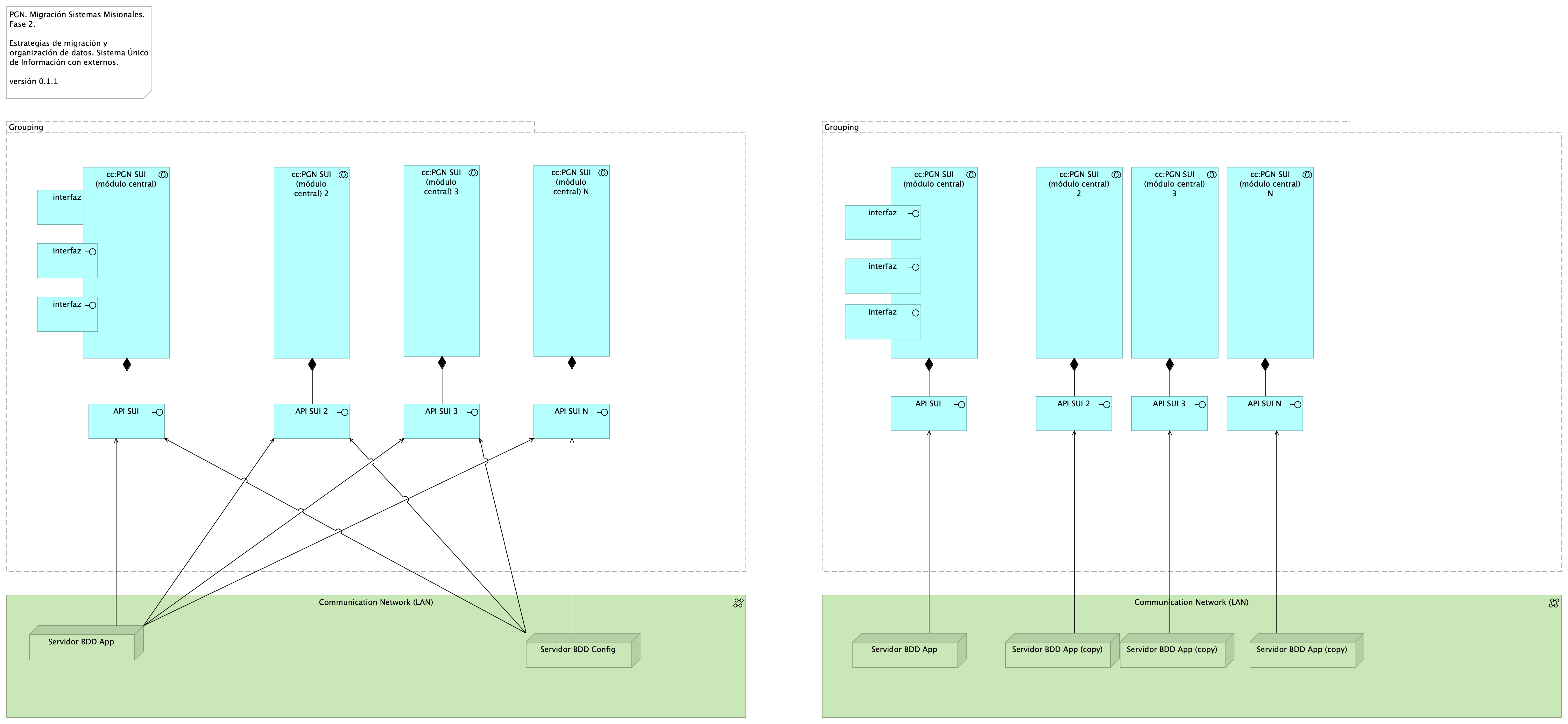


Imagen 14: Diagram: Migracion.6. Migración de datos

Modelo de acceso a datos de negocio del SIM.

La imagen siguiente presenta la organización de los ítems de transporte de datos de negocio necesarios para que los módulos del SUI puedan recolectar, procesar, integrar y almacenarlo de forma organizada y escalable.

Mediante esta organización, los datos de negocio son transportados desde sus respectivas fuentes mediante interfaces (principio de extensión y mantenibilidad referidos en las restricciones de la arquitecura del SUI Migrado). Los datos externos, entendidos como los de otros proveedores, son obtenidos mediante un intermediario: una API externa (*reverse proxy*).

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

### Catálogo de Elementos

| Name | Type | Description | Properties |
| --- | --- | --- | --- |
| **cc:PGN SUI (módulo central)** | application-collaboration | Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular de la PGN. |  |
| **cc:PGN SUI (módulo central)** | application-collaboration | Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular de la PGN. |  |
| **cc:PGN SUI (módulo central) 2** | application-collaboration | Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular de la PGN. |  |
| **cc:PGN SUI (módulo central) 2** | application-collaboration | Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular de la PGN. |  |
| **cc:PGN SUI (módulo central) 3** | application-collaboration | Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular de la PGN. |  |
| **cc:PGN SUI (módulo central) 3** | application-collaboration | Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular de la PGN. |  |
| **cc:PGN SUI (módulo central) N** | application-collaboration | Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular de la PGN. |  |
| **cc:PGN SUI (módulo central) N** | application-collaboration | Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular de la PGN. |  |
| **API SUI** | application-interface | API de representación del módulo. Centrlalización de la comunicación con otros módulos del SUI migrado. |  |
| **API SUI** | application-interface | API de representación del módulo. Centrlalización de la comunicación con otros módulos del SUI migrado. |  |
| **API SUI 2** | application-interface | API de representación del módulo. Centrlalización de la comunicación con otros módulos del SUI migrado. |  |
| **API SUI 2** | application-interface | API de representación del módulo. Centrlalización de la comunicación con otros módulos del SUI migrado. |  |
| **API SUI 3** | application-interface | API de representación del módulo. Centrlalización de la comunicación con otros módulos del SUI migrado. |  |
| **API SUI 3** | application-interface | API de representación del módulo. Centrlalización de la comunicación con otros módulos del SUI migrado. |  |
| **API SUI N** | application-interface | API de representación del módulo. Centrlalización de la comunicación con otros módulos del SUI migrado. |  |
| **API SUI N** | application-interface | API de representación del módulo. Centrlalización de la comunicación con otros módulos del SUI migrado. |  |
| **interfaz** | application-interface |  |  |
| **interfaz** | application-interface |  |  |
| **interfaz** | application-interface |  |  |
| **interfaz** | application-interface |  |  |
| **interfaz** | application-interface |  |  |
| **interfaz** | application-interface |  |  |
| **Communication Network (LAN)** | communication-network |  |  |
| **Communication Network (LAN)** | communication-network |  |  |
| **Grouping** | grouping |  |  |
| **Grouping** | grouping |  |  |
| **Servidor BDD App** | node | Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 GhzDiscos 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 App** | node | Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 GhzDiscos 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 App (copy)** | node | Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 GhzDiscos 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 App (copy)** | node | Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 GhzDiscos 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 App (copy)** | node | Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 GhzDiscos 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 GhzDiscos SO C: 80 GB, Backup E: 250 GB, SQL Data F: 250 GB, SQL Log G: 250 GB, TempDB G: 30 GB. |  |

# Organización Cambios Arquitectura

## Organización. 1n. Mapa producto



Imagen 15: Diagram: Organización. 1n. Mapa producto

### Catálogo de Elementos

| Name | Type | Description | Properties |
| --- | --- | --- | --- |
| **Épicas** | capability |  | *modulo:* |
| **Deliverable: (tiempo)** | deliverable |  | *modulo:* |
| **Tiempo** | gap |  |  |
| **Características** | goal |  | *modulo:* |
| **Hoja ruta del producto** | grouping |  | *modulo:* relatoria |
| **Hitos mercado** | value |  | *modulo:* |
| **Iteración** | work-package |  | *modulo:* |

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



Imagen 16: Diagram: Organización. 1n.1.b. Mapa producto PGN. Relatoría

### Catálogo de Elementos

| Name | Type | Description | Properties |
| --- | --- | --- | --- |
| **Administración de contenidos** | capability |  | *modulo:* relatoria |
| **Componente de comunicación segura SIU** | capability |  | *modulo:* conciliacion |
| **Componente de autenticación SIU** | capability |  | *modulo:* conciliacion |
| **Componente de autorización SIU** | capability |  | *modulo:* conciliacion |
| **Componentes de usabilidad, no. 1** | capability |  | *modulo:* relatoria |
| **Componentes de usabilidad, no. 2** | capability |  | *modulo:* relatoria |
| **Funcionalidades de búsqueda** | capability |  | *modulo:* relatoria |
| **Funcionalidades de descripción de contenidos** | capability |  | *modulo:* relatoria |
| **Integración API CMS** | capability |  | *modulo:* relatoria |
| **Motor de búsqueda** | capability |  | *modulo:* relatoria |
| **Proceso de organización de contenidos** | capability |  | *modulo:* relatoria |
| **Proceso de recolección de contenidos** | capability |  | *modulo:* relatoria |
| **Proceso de sincronización automática de contenidos** | capability |  | *modulo:* relatoria |
| **Épicas** | capability |  | *modulo:* |
| **Deliverable: (tiempo)** | deliverable |  | *modulo:* |
| **Autenticación** | goal |  | *modulo:* relatoria*caracteristica:* seguridad |
| **Autorización** | goal |  | *modulo:* relatoria*caracteristica:* seguridad |
| **Búsqueda** | goal |  | *modulo:* relatoria*caracteristica:* técnica, integración |
| **Características** | goal |  | *modulo:* |
| **Contenidos** | goal | Se tendran que adecuar los contenidos audivisuales de los sitios web, con subtitulos o CLosed Caption y la apropiacion de lenguajes de señas. | *modulo:* relatoria*caracteristica:* técnica, integración |
| **Descripción (metatada)** | goal |  | *modulo:* relatoria*caracteristica:* técnica, integración |
| **Indexación** | goal |  | *modulo:* relatoria*caracteristica:* técnica, integración |
| **Integridad** | goal |  | *modulo:* relatoria*caracteristica:* seguridad |
| **Recolección** | goal |  | *modulo:* relatoria*caracteristica:* técnica, integración |
| **Sincronización (actualizcn)** | goal |  | *modulo:* relatoria*caracteristica:* técnica, integración |
| **Usabilidad web** | goal |  | *modulo:* relatoria*caracteristica:* seguridad |
| **Usabilidad web** | goal |  | *modulo:* relatoria*caracteristica:* seguridad |
| **Hoja ruta del producto** | grouping |  | *modulo:* relatoria |
| **Adopción, v1.2** | value |  | *modulo:* relatoria |
| **Búsqueda de contenidos. Relatoría v0.1** | value |  | *modulo:* relatoria |
| **Despliegue Relatoría v1.2** | value |  | *modulo:* relatoria |
| **Gestión contenidos. Rltría v1.0** | value |  | *modulo:* relatoria |
| **Hitos mercado** | value |  | *modulo:* |
| **Organización contenidos. Rltría v0.5** | value |  | *modulo:* relatoria |
| **Iteración** | work-package |  | *modulo:* |
| **Iteración 2** | work-package |  | *modulo:* relatoria |
| **Iteración 3** | work-package |  | *modulo:* relatoria |
| **Iteración 4** | work-package |  | *modulo:* relatoria |
| **Iteración 5** | work-package |  | *modulo:* relatoria |
| **Iteración 6** | work-package |  | *modulo:* relatoria |
| **Iteración 7** | work-package |  | *modulo:* relatoria |
| **rel.Iteración 1** | work-package |  | *modulo:* relatoria |

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



Imagen 17: Diagram: Organización. 2n.1a. Mapa producto PGN. Conciliacion

### Catálogo de Elementos

| Name | Type | Description | Properties |
| --- | --- | --- | --- |
| **Componente de comunicación segura SIU** | capability |  | *modulo:* conciliacion |
| **Componente de autenticación SIU** | capability |  | *modulo:* conciliacion |
| **Componente de autorización SIU** | capability |  | *modulo:* conciliacion |
| **Flujo de trabajo Preventico** | capability |  | *modulo:* conciliacion |
| **Flujo de trabajo Disciplinar** | capability |  | *modulo:* conciliacion |
| **Flujo de trabajo Intervención** | capability |  | *modulo:* conciliacion |
| **Integración API Dokus** | capability |  | *modulo:* conciliacion |
| **Motor de flujo de trabajo** | capability |  | *modulo:* conciliacion |
| **Panel de control flujos** | capability |  | *modulo:* conciliacion |
| **Reporte flujos de trabajo** | capability |  | *modulo:* conciliacion |
| **Épicas** | capability |  | *modulo:* |
| **Deliverable: (tiempo)** | deliverable |  | *modulo:* |
| **Autenticación** | goal |  | *modulo:* conciliacion*caracteristica:* seguridad |
| **Autorización** | goal |  | *modulo:* conciliacion*caracteristica:* seguridad |
| **Características** | goal |  | *modulo:* |
| **Conciliación administrativa** | goal |  | *modulo:* conciliacion*caracteristica:* técnica, integración |
| **Conciliación civil** | goal |  | *modulo:* conciliacion*caracteristica:* técnica, integración |
| **Conciliación disciplinar** | goal |  | *modulo:* conciliacion*caracteristica:* técnica, integración |
| **Conciliación familia** | goal |  | *modulo:* conciliacion*caracteristica:* técnica, integración |
| **Conciliación preventivo** | goal |  | *modulo:* conciliacion*caracteristica:* técnica, integración |
| **Diseño de flujos de Conciliación** | goal |  | *modulo:* conciliacion*caracteristica:* técnica, integración |
| **Gestión de instancias (flujos)** | goal |  | *modulo:* conciliacion*caracteristica:* técnica, integración |
| **Gestión documental** | goal |  | *modulo:* conciliacion*caracteristica:* seguridad |
| **Informes de gestión flujos** | goal |  | *modulo:* conciliacion*caracteristica:* técnica, integración |
| **Integridad** | goal |  | *modulo:* conciliacion*caracteristica:* seguridad |
| **Hoja ruta del producto** | grouping |  | *modulo:* relatoria |
| **Adopción, v1.2** | value |  | *modulo:* conciliacion |
| **Despliegue Conciliación v1.2** | value |  | *modulo:* conciliacion |
| **Flujo de trabajo Disciplinario. Conciliación v0.9** | value |  | *modulo:* conciliacion |
| **Flujo de trabajo Intervención. Conciliación v0.1 (copy)** | value |  | *modulo:* conciliacion |
| **Flujo de trabajo Preventivo. Conciliación v0.7** | value |  | *modulo:* conciliacion |
| **Gestión de flujos. Conciliación 1.0** | value |  | *modulo:* conciliacion |
| **Hitos mercado** | value |  | *modulo:* |
| **Iteración** | work-package |  | *modulo:* |
| **Iteración 1** | work-package |  | *modulo:* conciliacion |
| **Iteración 2** | work-package |  | *modulo:* conciliacion |
| **Iteración 3** | work-package |  | *modulo:* conciliacion |
| **Iteración 4** | work-package |  | *modulo:* conciliacion |
| **Iteración 5** | work-package |  | *modulo:* conciliacion |
| **Iteración 6** | work-package |  | *modulo:* conciliacion |
| **Iteración 7** | work-package |  | *modulo:* conciliacion |

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



Imagen 18: Diagram: Organización. 4n.1. Mapa producto PGN. Estratego

### Catálogo de Elementos

| Name | Type | Description | Properties |
| --- | --- | --- | --- |
| **Épicas** | capability |  | *modulo:* |
| **Épicas** | capability |  | *modulo:* estratego |
| **Épicas** | capability |  | *modulo:* estratego |
| **Épicas** | capability |  | *modulo:* estratego |
| **Épicas** | capability |  | *modulo:* estratego |
| **Épicas** | capability |  | *modulo:* estratego |
| **Épicas** | capability |  | *modulo:* estratego |
| **Deliverable: (tiempo)** | deliverable |  | *modulo:* |
| **Acciones correctivas** | goal | Administrar los riesgos asociados a cada uno de los indicadores o planes. | *modulo:* estratego |
| **Auditoria de mediciones** | goal | Gestionar las actividades de los usuarios, como el registro de indicadores, el tipo, etc. | *modulo:* estratego |
| **Auditorias** | goal | Gestionar el control de logs de las actividades realizadas por el usuario en sesión. | *modulo:* estratego |
| **Características** | goal |  | *modulo:* |
| **Dependencias** | goal | Reportar al sistema, actividades, proyectos, indicadores. | *modulo:* estratego |
| **Grupos (Roles)** | goal | Administrar los roles y permisos dentro del sistema | *modulo:* estratego |
| **Gráficos** | goal | Generar y presentar gráficos | *modulo:* estratego |
| **Históricos** | goal | Almacenar y consultar históricos dentro del sistema | *modulo:* estratego |
| **Informes** | goal | Generar documentos con los informes correspondientes. | *modulo:* estratego |
| **Instrumento de cooperación** | goal | Administrar los proyectos de los cooperantes. | *modulo:* estratego |
| **Organizaciones** | goal | Estructura principal. | *modulo:* estratego |
| **Planes administrar** | goal | Administrar el plan estratégico institucional. | *modulo:* estratego |
| **Planes asociar** | goal | Asociar recursos, presupuesto. | *modulo:* estratego |
| **Planes generar** | goal | Generar planes estratégicos institucionales y asociar los planes de acción preventivos. | *modulo:* estratego |
| **Portafolio** | goal | Gestionar el portafolio de todos los proyectos de la entidad. | *modulo:* estratego |
| **Reportes** | goal | Generar reportes y exportarlos en diferentes tipos de archivo. | *modulo:* estratego |
| **Usuarios** | goal | Administrar los usuarios del sistema | *modulo:* estratego |
| **Hoja ruta del producto** | grouping |  | *modulo:* relatoria |
| **Hitos mercado** | value |  | *modulo:* |
| **Hitos mercado** | value |  | *modulo:* estratego |
| **Hitos mercado** | value |  | *modulo:* estratego |
| **Hitos mercado** | value |  | *modulo:* estratego |
| **Hitos mercado** | value |  | *modulo:* estratego |
| **Iteración** | work-package |  | *modulo:* |
| **Iteración** | work-package |  | *modulo:* estratego |
| **Iteración** | work-package |  | *modulo:* estratego |
| **Iteración** | work-package |  | *modulo:* estratego |
| **Iteración** | work-package |  | *modulo:* estratego |
| **Iteración 1** | work-package |  | *modulo:* estratego |
| **Iteración 6** | work-package |  | *modulo:* estratego |

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



Imagen 19: Diagram: Organización. 3n.1. Mapa producto PGN. SIAF

### Catálogo de Elementos

| Name | Type | Description | Properties |
| --- | --- | --- | --- |
| **Épicas** | capability |  | *modulo:* |
| **Épicas** | capability |  | *modulo:* siaf |
| **Épicas** | capability |  | *modulo:* siaf |
| **Épicas** | capability |  | *modulo:* siaf |
| **Épicas** | capability |  | *modulo:* siaf |
| **Épicas** | capability |  | *modulo:* siaf |
| **Épicas** | capability |  | *modulo:* siaf |
| **Épicas** | capability |  | *modulo:* siaf |
| **Épicas** | capability |  | *modulo:* siaf |
| **Épicas (copy) (copy) (copy) (copy)** | capability |  | *modulo:* siaf |
| **Deliverable: (tiempo)** | deliverable |  | *modulo:* |
| **Acciones de acuerdo al estado** | goal | Realización de acciones específicas según el estado de los movimientos devolutivos. | *modulo:* siaf |
| **Almacén** | goal | Administración de almacenes. | *modulo:* siaf |
| **Asientos** | goal | Registro de asientos. | *modulo:* siaf |
| **CRUD Campos** | goal | Operaciones CRUD (Crear, Leer, Actualizar, Eliminar) en campos de los asientos. | *modulo:* siaf |
| **Características** | goal |  | *modulo:* |
| **Creación de movimiento** | goal | Generación de movimientos de acuerdo con los asientos abiertos. | *modulo:* siaf |
| **Cuenta de funcionario** | goal | Gestión de cuentas de funcionarios. | *modulo:* siaf |
| **Cuenta en Microsoft (Autenticación)** | goal | Autenticación mediante cuentas de Microsoft. | *modulo:* siaf |
| **Cálculo de total** | goal | Cálculo automático del total basado en la información de elementos. | *modulo:* siaf |
| **Código (autoincremental)** | goal | Generación automática de códigos que se reinician cada año. | *modulo:* siaf |
| **Dependiendo del tipo de movimiento** | goal | Gestión de movimientos según su tipo, incluyendo elementos como conceptos, beneficiarios y funcionarios (maestros). | *modulo:* siaf |
| **Elementos** | goal | Registro de elementos relacionados con los movimientos. | *modulo:* siaf |
| **Estado** | goal | Seguimiento del estado de los asientos. | *modulo:* siaf |
| **Fecha automática** | goal | Asignación automática de la fecha en los asientos. | *modulo:* siaf |
| **Filtrar por campos** | goal | Capacidad para filtrar los movimientos devolutivos según campos específicos. | *modulo:* siaf |
| **Funcionario Posesionado** | goal | Registro de información sobre funcionarios en posesión. | *modulo:* siaf |
| **Funcionarios (Nómina) vs Funcionarios (Siaf)** | goal | Comparación y actualización de información de funcionarios almacenada en Siaf con la información de nómina. | *modulo:* siaf |
| **Generar documento** | goal | Creación de documentos relacionados con los movimientos. | *modulo:* siaf |
| **Generar reportes** | goal | Creación de informes y reportes para proporcionar la información solicitada. | *modulo:* siaf |
| **Login (Doble factor)** | goal | Autenticación de usuario mediante doble factor de seguridad | *modulo:* siaf |
| **Movimiento Consumible** | goal | Registro de movimientos relacionados con elementos consumibles. | *modulo:* siaf |
| **Movimiento devolutivo** | goal | Registro de movimientos devolutivos. | *modulo:* siaf |
| **Sincronización con Homminis** | goal | Sincronización de datos con el sistema Homminis. | *modulo:* siaf |
| **Vista CRUD** | goal | Interfaz para crear, leer, actualizar y eliminar registros en el almacén. | *modulo:* siaf |
| **Vista formulario personalizada** | goal | Personalización de formularios para la creación de asientos dependiendo del almacén. | *modulo:* siaf |
| **Vista tipo formulario personalizada** | goal | Personalización de formularios para ingresar datos relacionados con los asientos. | *modulo:* siaf |
| **Vista tipo lista personalizada** | goal | Visualización personalizada en forma de lista con filtros por campos específicos. | *modulo:* siaf |
| **Hoja ruta del producto** | grouping |  | *modulo:* relatoria |
| **Hitos mercado** | value |  | *modulo:* |
| **Hitos mercado** | value |  | *modulo:* siaf |
| **Hitos mercado** | value |  | *modulo:* siaf |
| **Hitos mercado** | value |  | *modulo:* siaf |
| **Hitos mercado** | value |  | *modulo:* siaf |
| **Iteración** | work-package |  | *modulo:* |
| **Iteración 1** | work-package |  | *modulo:* siaf |
| **Iteración 1** | work-package |  | *modulo:* siaf |
| **Iteración 1** | work-package |  | *modulo:* siaf |
| **Iteración 1** | work-package |  | *modulo:* siaf |
| **Iteración 1** | work-package |  | *modulo:* siaf |
| **Iteración 1** | work-package |  | *modulo:* siaf |
| **Iteración 1** | work-package |  | *modulo:* siaf |
| **Iteración 1** | work-package |  | *modulo:* siaf |
| **Iteración 9** | work-package |  | *modulo:* siaf |

# Arquitectura de Seguridad, SUI Migración

## Seguridad.1. Requerimientos



Imagen 20: Diagram: Seguridad.1. Requerimientos

### Catálogo de Elementos

| Name | Type | Description | Properties |
| --- | --- | --- | --- |
| **cc:Administración** | application-collaboration |  |  |
| **cc:PGN SUI (módulo central)** | application-collaboration | Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular de la PGN. |  |
| **interfaz** | application-interface |  |  |
| **interfaz** | application-interface |  |  |
| **interfaz** | application-interface |  |  |
| **interfaz** | application-interface |  |  |
| **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 validos 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,requirementRQRSEG11,“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 frente apruebas 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, maquina, 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. |  |

## Seguridad. Linebase.2.Portal



Imagen 21: Diagram: Seguridad. 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 Procuraduría.

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

### Catálogo de Elementos

| Name | Type | Description | Properties |
| --- | --- | --- | --- |
| **Application Collaboration Sharepoint** | application-collaboration |  |  |
| **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 autenticacion del directorio activo, y la integración del Single Sign-On (SSO), con el inicio unico 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 informacion 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 |  |  |
| **Application Interface** | application-interface |  |  |

# Análisis de Productos

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



Imagen 22: Diagram: Organización. 4n.1a. Mapa producto PGN. Comparativa

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 ejecuta 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 operativos de inventario de SIAF. Basado en esto, Estratego reporta mayor beneficio y menos impacto en esfuerzo (por la razón anterior) que SIAF.

En conclusion, 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.

### Catálogo de Elementos

| Name | Type | Description | Properties |
| --- | --- | --- | --- |
| **Épicas** | capability |  | *modulo:* estratego |
| **Épicas** | capability |  | *modulo:* estratego |
| **Épicas** | capability |  | *modulo:* estratego |
| **Épicas** | capability |  | *modulo:* estratego |
| **Épicas** | capability |  | *modulo:* estratego |
| **Épicas** | capability |  | *modulo:* estratego |
| **Épicas (copy)** | capability |  | *modulo:* siaf |
| **Épicas (copy)** | capability |  | *modulo:* siaf |
| **Épicas (copy)** | capability |  | *modulo:* siaf |
| **Épicas (copy)** | capability |  | *modulo:* siaf |
| **Épicas (copy)** | capability |  | *modulo:* siaf |
| **Épicas (copy)** | capability |  | *modulo:* siaf |
| **Épicas (copy)** | capability |  | *modulo:* siaf |
| **Épicas (copy)** | capability |  | *modulo:* siaf |
| **Épicas (copy) (copy) (copy) (copy) (copy)** | capability |  | *modulo:* siaf |
| **Acciones correctivas** | goal | Administrar los riesgos asociados a cada uno de los indicadores o planes. | *modulo:* estratego |
| **Acciones de acuerdo al estado (copy)** | goal | Realización de acciones específicas según el estado de los movimientos devolutivos. | *modulo:* siaf |
| **Almacén (copy)** | goal | Administración de almacenes. | *modulo:* siaf |
| **Asientos (copy)** | goal | Registro de asientos. | *modulo:* siaf |
| **Auditoria de mediciones** | goal | Gestionar las actividades de los usuarios, como el registro de indicadores, el tipo, etc. | *modulo:* estratego |
| **Auditorias** | goal | Gestionar el control de logs de las actividades realizadas por el usuario en sesión. | *modulo:* estratego |
| **CRUD Campos (copy)** | goal | Operaciones CRUD (Crear, Leer, Actualizar, Eliminar) en campos de los asientos. | *modulo:* siaf |
| **Creación de movimiento (copy)** | goal | Generación de movimientos de acuerdo con los asientos abiertos. | *modulo:* siaf |
| **Cuenta de funcionario (copy)** | goal | Gestión de cuentas de funcionarios. | *modulo:* siaf |
| **Cuenta en Microsoft (Autenticación) (copy)** | goal | Autenticación mediante cuentas de Microsoft. | *modulo:* siaf |
| **Cálculo de total (copy)** | goal | Cálculo automático del total basado en la información de elementos. | *modulo:* siaf |
| **Código (autoincremental) (copy)** | goal | Generación automática de códigos que se reinician cada año. | *modulo:* siaf |
| **Dependencias** | goal | Reportar al sistema, actividades, proyectos, indicadores. | *modulo:* estratego |
| **Dependiendo del tipo de movimiento (copy)** | goal | Gestión de movimientos según su tipo, incluyendo elementos como conceptos, beneficiarios y funcionarios (maestros). | *modulo:* siaf |
| **Elementos** | goal | Registro de elementos relacionados con los movimientos. | *modulo:* siaf |
| **Estado (copy)** | goal | Seguimiento del estado de los asientos. | *modulo:* siaf |
| **Fecha automática (copy)** | goal | Asignación automática de la fecha en los asientos. | *modulo:* siaf |
| **Filtrar por campos (copy)** | goal | Capacidad para filtrar los movimientos devolutivos según campos específicos. | *modulo:* siaf |
| **Funcionario Posesionado (copy)** | goal | Registro de información sobre funcionarios en posesión. | *modulo:* siaf |
| **Funcionarios (Nómina) vs Funcionarios (Siaf) (copy)** | goal | Comparación y actualización de información de funcionarios almacenada en Siaf con la información de nómina. | *modulo:* siaf |
| **Generar documento (copy)** | goal | Creación de documentos relacionados con los movimientos. | *modulo:* siaf |
| **Generar reportes (copy)** | goal | Creación de informes y reportes para proporcionar la información solicitada. | *modulo:* siaf |
| **Grupos (Roles)** | goal | Administrar los roles y permisos dentro del sistema | *modulo:* estratego |
| **Gráficos** | goal | Generar y presentar gráficos | *modulo:* estratego |
| **Históricos** | goal | Almacenar y consultar históricos dentro del sistema | *modulo:* estratego |
| **Informes** | goal | Generar documentos con los informes correspondientes. | *modulo:* estratego |
| **Instrumento de cooperación** | goal | Administrar los proyectos de los cooperantes. | *modulo:* estratego |
| **Login (Doble factor) (copy)** | goal | Autenticación de usuario mediante doble factor de seguridad | *modulo:* siaf |
| **Movimiento Consumible (copy)** | goal | Registro de movimientos relacionados con elementos consumibles. | *modulo:* siaf |
| **Movimiento devolutivo (copy)** | goal | Registro de movimientos devolutivos. | *modulo:* siaf |
| **Organizaciones** | goal | Estructura principal. | *modulo:* estratego |
| **Planes administrar** | goal | Administrar el plan estratégico institucional. | *modulo:* estratego |
| **Planes asociar** | goal | Asociar recursos, presupuesto. | *modulo:* estratego |
| **Planes generar** | goal | Generar planes estratégicos institucionales y asociar los planes de acción preventivos. | *modulo:* estratego |
| **Portafolio** | goal | Gestionar el portafolio de todos los proyectos de la entidad. | *modulo:* estratego |
| **Reportes** | goal | Generar reportes y exportarlos en diferentes tipos de archivo. | *modulo:* estratego |
| **Sincronización con Homminis (copy)** | goal | Sincronización de datos con el sistema Homminis. | *modulo:* siaf |
| **Usuarios** | goal | Administrar los usuarios del sistema | *modulo:* estratego |
| **Vista CRUD (copy)** | goal | Interfaz para crear, leer, actualizar y eliminar registros en el almacén. | *modulo:* siaf |
| **Vista formulario personalizada (copy)** | goal | Personalización de formularios para la creación de asientos dependiendo del almacén. | *modulo:* siaf |
| **Vista tipo formulario personalizada (copy)** | goal | Personalización de formularios para ingresar datos relacionados con los asientos. | *modulo:* siaf |
| **Vista tipo lista personalizada (copy)** | goal | Visualización personalizada en forma de lista con filtros por campos específicos. | *modulo:* siaf |
| **Hitos mercado** | value |  | *modulo:* estratego |
| **Hitos mercado** | value |  | *modulo:* estratego |
| **Hitos mercado** | value |  | *modulo:* estratego |
| **Hitos mercado** | value |  | *modulo:* estratego |
| **Hitos mercado** | value |  | *modulo:* siaf |
| **Hitos mercado** | value |  | *modulo:* siaf |
| **Hitos mercado** | value |  | *modulo:* siaf |
| **Hitos mercado** | value |  | *modulo:* siaf |
| **Iteración** | work-package |  | *modulo:* estratego |
| **Iteración** | work-package |  | *modulo:* estratego |
| **Iteración** | work-package |  | *modulo:* estratego |
| **Iteración** | work-package |  | *modulo:* estratego |
| **Iteración 1** | work-package |  | *modulo:* estratego |
| **Iteración 1 (copy)** | work-package |  | *modulo:* siaf |
| **Iteración 1 (copy)** | work-package |  | *modulo:* siaf |
| **Iteración 1 (copy)** | work-package |  | *modulo:* siaf |
| **Iteración 1 (copy)** | work-package |  | *modulo:* siaf |
| **Iteración 1 (copy)** | work-package |  | *modulo:* siaf |
| **Iteración 1 (copy)** | work-package |  | *modulo:* siaf |
| **Iteración 1 (copy)** | work-package |  | *modulo:* siaf |
| **Iteración 1 (copy)** | work-package |  | *modulo:* siaf |
| **Iteración 6** | work-package |  | *modulo:* estratego |
| **Iteración 9 (copy)** | work-package |  | *modulo:* siaf |

# Riesgos Técnicos

## Riesgos.1. Migración funcional



Imagen 23: Diagram: 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
* RSG11. Estrategias de Migración de datos
* RSG12. Arquitectura de almancenamiento y distribución de datos SIU
* RSG13. Sistema de autenticación híbrido

### 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.

### Catálogo de Elementos

| Name | Type | Description | Properties |
| --- | --- | --- | --- |
| **RSG1. Estrategia CMS central** | constraint | Establecer desde el principio el gestor de contenidos compartido que los módulos del SUI migrados van a usar. |  |
| **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 incluídas en contrato 078, Migración Funcional SIU en atención al numeral 5.6 del anexo técnico del proyecto. | 5.6 MIGRACIÓN DE DATOS |
| **RSG12. Arquitectura de almancenamiento y distribución de datos SIU** | constraint | Definir la opción de organización y distribución de los almacenes de datos del SIU. opc1. Dispositivo físico/virtual (nodo, servidor, y esquema de base de datos) único, central, a todos los módulos del SIU.opc2. Dispositivos virtuales autónomos por dominio de negocio: rlatoría, inventario, información estratégica, intercomunicados. |  |
| **RSG13. Sistema de autenticación híbrido** | constraint | Definir la estrategia de autenticación del SIU migrado (aplicable a todos los módulos del SIU migrado).opc1. Híbrida: integrado, directorio empresarial (LDAP), y servicios de autenticación de confianza: Office 365 de PGN.opc2. Servicio de autenticación de confianza: Office 365 de PGN. |  |
| **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 Estratego 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 estrcturales 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 AccesoLos 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 autorizadosLos 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. |  |

## Riesgos.2. Modelo Riesgo RSG10



Imagen 24: Diagram: Riesgos.2. Modelo Riesgo RSG10

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 4: 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. |

### Catálogo de Elementos

| Name | Type | Description | Properties |
| --- | --- | --- | --- |
| **Impacto** | assessment |  |  |
| **Agente de riesgo PGN** | business-actor | Arquitecto PGN |  |
| **Agente de riesgo Softgic** | business-actor | Arquitecto Softgic |  |
| **Desconocimiento arq. de referencia SUI** | business-event |  |  |
| **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. |  |
| **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. |  |
| **Definición tipos de datos módulos SUI** | requirement |  |  |
| **Supervisor contrato 078-2023** | stakeholder |  |  |

Generated on: Tue Nov 07 2023 23:59:58 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. Para los casos que aplique se debe asociar el desarrollo con el mecanismo de Firmas (digital, electrónica o mecánica): Esta funcionalidad debe permitir configurar los usuarios que tienen permitida la aprobación de documentos desde la solución implementada, a través del tipo de firma que corresponda.
4. Administrar los Permisos de acceso: Esta funcionalidad permite definir específicamente a que servicios de la solución puede ingresar un usuario (CRUD).
5. 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.
6. Las soluciones deben permitir la configuración de permisos de consulta con diferentes alcances para cada tipo de usuario.
7. Desde la interfaz de usuario se debe poder crear, modificar o inactivar usuarios, perfiles o roles, permisos a las diferentes funcionalidades de la solución.
8. Las soluciones deben permitir la definición de varios tipos de usuario.
9. Las soluciones deben permitir la parametrización de los consecutivos que maneja la entidad para los diferentes documentos generados por las soluciones.
10. Debe permitir parametrizar la vinculación del consecutivo a un documento en forma manual o automática.
11. 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, maquina, 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 apruebas 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”.

# Anexos

## Modelo ER del SIU Migrado

Documento vista modelo físico de datos (modelo ER, entidad-relación) del Sistema Único de Información (SUI).

# Referencias

[[1](#ref-19ZPD5YjC)] [[2](#ref-hQTPO0iI)] [[3](#ref-l0mriBft)] [[**eservices5-23?**](#ref-eservices5-23)] [[**eservices6-12?**](#ref-eservices6-12)] [[**eservices7-23?**](#ref-eservices7-23)] [[**bptrends07?**](#ref-bptrends07)]

1. **Softgic. Proyecto de mejoramiento SIU de PGN. Fase i** Softgic, PGN (2022-06) <https://hwong23.github.io/fna-devdoc-f1/v/6497aef0f15c3591f0728e4c42cb2c26c13b43aa/>

2. **Procuraduría general de la nación. Anexo - especificaciones técnicas 19-05-2023** PGN (2023-05) <https://hwong23.github.io/fna-devdoc-f1/v/6497aef0f15c3591f0728e4c42cb2c26c13b43aa/>

3. **PGN manual técnico sharepoint, versión 1** Softgic, PGN (2022-05) <https://hwong23.github.io/fna-devdoc-f1/v/6497aef0f15c3591f0728e4c42cb2c26c13b43aa/>