

Documento de Arquitectura Migración Funcional PGN SIU

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

Versión del producto 1.81a9f10 de 21 Oct 2023

Presentado a

Procuraduría General de la Nación (PGN)

Fecha

21 Oct 2023

Autores

- **Harry Wong, ing.**
·  Usuario [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	1.81a9f10 del 21 Oct 2023

git show -s -n 4 | Vínculos | [N003a Vista Segmento PGN SIU](#) |

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 preventiva 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 relatoria, 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 redundará 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.

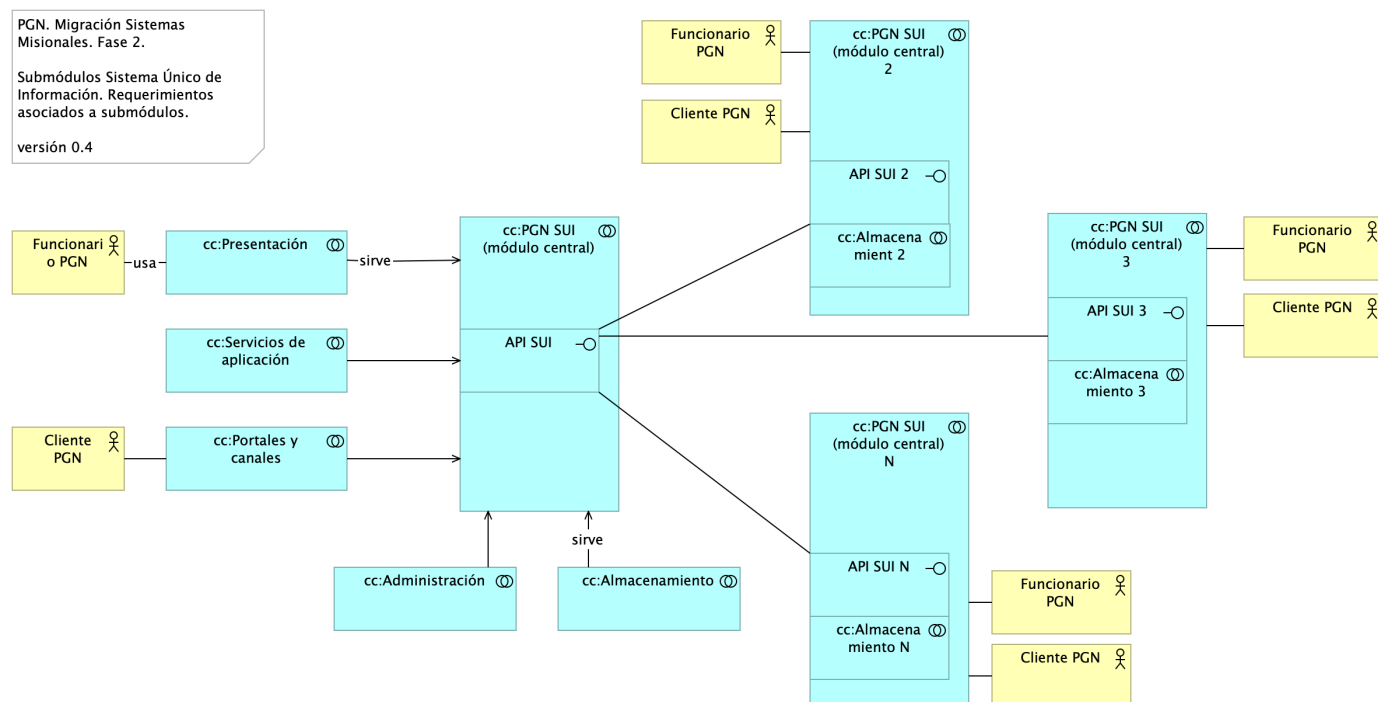
Requisito	Extensibilidad SUI
Descripción	Concentración de los componentes de negocio, misionales, del SUI protegidos de cambios provenientes de otros sistemas. Ver Patrón de Diseño Migración SUI, más adelante en el documento.
Calidad sistémica	La extensibilidad que optimiza el diseño Migración SUI está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

Arquitectura de Software

- Diagrama de Arquitectura de la Solución Propuesta: vista de integración
 - Migracion.1a.a.SIU Contexto
 - Migracion.1a.b.SIU Módulos
- Diagrama de Arquitectura de la solución propuesta: vista física
 - Lineabase.0.SIU aplicación. física
- Diagrama de Arquitectura de la Solución Propuesta: motivadores del negocio
 - Migracion.1a.b.SIU Módulos
 - Riesgos.1. Migración funcional
 - Riesgos.2. Modelo Riesgo RSG10
 - Riesgos.3. Modelo Riesgo RSG11
- Diagrama de Arquitectura de la Solución Propuesta: interoperabilidad
 - Migracion.1c.SIU Modulos Colaboración
- Diagrama de Arquitectura de la Solución Propuesta: gestión de autenticación, usuarios y roles
 - Seguridad.2. Lineabase.0.SIU Aplicación
- Diagrama de Clases y Componentes de solución
 - Migracion.1b.1. SIU Módulos Componentes
 - Migracion.1b.2. SIU Módulos Componentes. Brecha
- Diagrama de Arquitectura de Integración Continua, Devops y Despliegues de Capas
 - Migracion.4. CI
- Documento de Relación de Tecnologías y Licenciamiento
 - Migracion.5. Licenciamiento

Diagrama de Arquitectura de la Solución Propuesta: vista de integración

Migracion.1a.a.SIU Contexto



RQR.	Requerimiento contractual
ARQ.	Restricción de arquitectura

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

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

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

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

Catálogo de Elementos

Name	Type	Description	Properties
cc:Administración	application-collaboration		
cc:Almacenamient 2	application-collaboration	Espacio de almacenamiento operativo y transaccional de un módulo central del SUI migrado.	
cc:Almacenamiento	application-collaboration	Espacio de almacenamiento operativo y transaccional de un módulo central del SUI migrado.	
cc:Almacenamiento 3	application-collaboration	Espacio de almacenamiento operativo y transaccional de un módulo central del SUI migrado.	
cc:Almacenamiento N	application-collaboration	Espacio de almacenamiento operativo y transaccional de un módulo central del SUI migrado.	
cc:PGN SUI (módulo central)	application-collaboration	Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular de la PGN.	

Name	Type	Description	Properties
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) N	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.	
API SUI	application-interface	API de representación del módulo. Centralización de la comunicación con otros módulos del SUI migrado.	
API SUI 2	application-interface	API de representación del módulo. Centralización de la comunicación con otros módulos del SUI migrado.	
API SUI 3	application-interface	API de representación del módulo. Centralización de la comunicación con otros módulos del SUI migrado.	
API SUI N	application-interface	API de representación del módulo. Centralización de la comunicación con otros módulos del SUI migrado.	
Cliente PGN	business-actor		
Cliente PGN	business-actor		
Cliente PGN	business-actor		
Cliente PGN	business-actor		
Funcionario PGN	business-actor		
Funcionario PGN	business-actor		
Funcionario PGN	business-actor		
Funcionario PGN	business-actor		

Migracion.1a.b.SIU Módulos

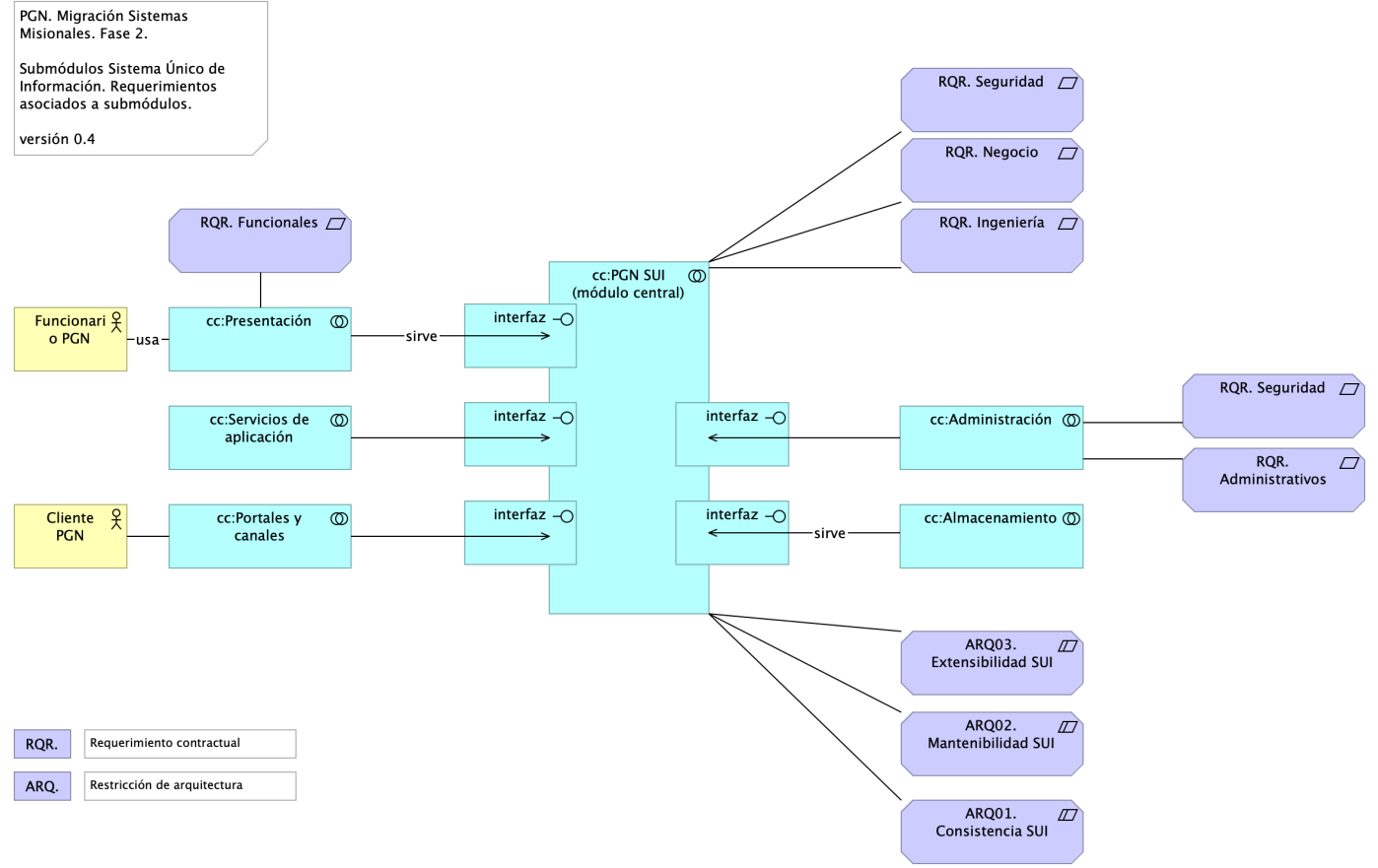


Imagen 2: Diagram: Migracion.1a.b.SIU Módulos

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 almacenamiento operativo y transaccional de un módulo central del SUI migrado.	
cc:PGN SUI (módulo central)	application-collaboration	Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular de la PGN.	

Name	Type	Description	Properties
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 redundará 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.	

Diagrama de Arquitectura de la solución propuesta: vista física

Lineabase.0.SIU aplicación. física

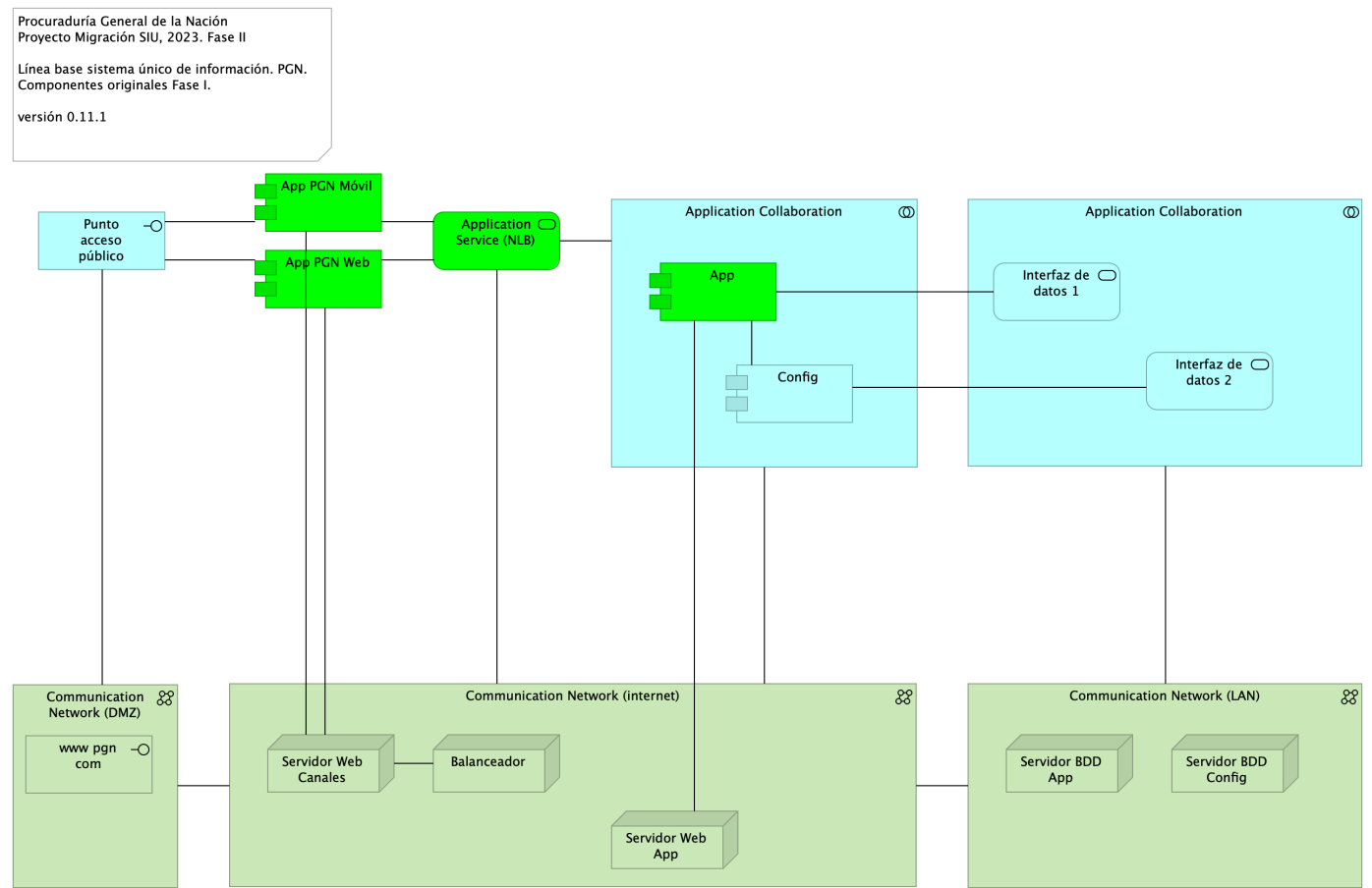


Imagen 3: Diagram: Lineabase.0.SIU aplicación. física

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

Representación Arquitectónica

Con una arquitectura orientada a servicios SUI recopila:

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

Catálogo de Elementos

Name	Type	Description	Properties
Application Collaboration	application-collaboration		
Application Collaboration	application-collaboration		
App	application-component		plataforma: node Js brecha: 100

Name	Type	Description	Properties
App PGN Móvil	application-component	<p>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.</p> <p>Protección de datos personales,</p> <p>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.</p> <p>La informacion contenida en las bases de datos debe tener los mecanismos de cifrado que en otros apartados se han mencionado.</p> <p>La legislación que hay que tener como referencia, ley 1581 de 2012. Decreto 1377 de 2013</p> <p>La metodologia empleada tendrá las siguientes fases:</p> <ul style="list-style-type: none">• FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como: o Recopilación de dominios/IPs/puertos/servicios o Recopilación de metadatos o Uso de Google Dorks.• ANÁLISIS DE VULNERABILIDADES: Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.• EXPLOTACIÓN: • Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo: o Inyección de código o Inclusión de ficheros locales o remotos o Evasión de autenticación o Carencia de controles de autorización o Ejecución de comandos en el lado del servidor o Ataques tipo Cross Site Request Forgery o Control de errores o Gestión de sesiones o Fugas de información o Secuestros de sesión o Comprobación de las condiciones para realizar una denegación de servicio.• POST EXPLOTACIÓN: En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adiciones con el objetivo de comprobar la criticidad de esta. No URL IP 1. https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz 135.181.185.207	<p><i>plantilla: element-md-bold</i> <i>brecha: 100</i></p>

Name	Type	Description	Properties
App PGN Web	application-component	<p>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 Ethical Hacking.</p> <p>Los resultados permitirán identificar los requisitos de seguridad que los sistemas de informacion o servicios web deberán cumplir.</p> <p>La metodologia empleada tendrá las siguientes fases:</p> <ul style="list-style-type: none"> • FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como: o Recopilación de dominios/IPs/puertos/servicios o Recopilación de metadatos o Uso de Google Dorks. • ANÁLISIS DE VULNERABILIDADES: Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades. • EXPLOTACIÓN: • Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo: o Inyección de código o Inclusión de ficheros locales o remotos o Evasión de autenticación o Carencia de controles de autorización o Ejecución de comandos en el lado del servidor o Ataques tipo Cross Site Request Forgery o Control de errores o Gestión de sesiones o Fugas de información o Secuestros de sesión o Comprobación de las condiciones para realizar una denegación de servicio. • POST EXPLOTACIÓN: En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adiciones con el objetivo de comprobar la criticidad de esta. No URL IP 1. https://runtimeptest.lappiz.io/#/auth/login/ PGN_Lappiz 135.181.185.207 El Login deberá evidenciar el control de errores, al momento de realizar la validación deberá mensaje de error para el caso que se autentique con credenciales erradas. 	<p>plataforma: angular 11 brecha: 100</p>
Config	application-component		plataforma: cs
Punto acceso público	application-interface	URL tipo C HTTP	
Application Service (NLB)	application-service		plataforma: angular 11 brecha: 100
Interfaz de datos 1	application-service		
Interfaz de datos 2	application-service		
Communication Network (DMZ)	communication-network		
Communication Network (LAN)	communication-network		
Communication Network (internet)	communication-network		
Balanceador	node		
Servidor BDD App	node	Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz Discos SO C: 126 GB, Backup E: 511 GB, SQL Data F: 510 GB, SQL Log G: 510 GB, TempDB G: 63.6 GB.	
Servidor BDD Config	node	Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz Discos SO C: 80 GB, Backup E: 250 GB, SQL Data F: 250 GB, SQL Log G: 250 GB, TempDB G: 30 GB.	

Name	Type	Description	Properties
Servidor Web App	node	Windows Server 2019 Standard o Datacenter x64. Nombre físico. IP LAN. IP Pública. Windows Server 2019 Standard or Datacenter x64. RAM 8 GB. CPU 64 Bits. 4 Cores de 2 Ghz. Discos SO C: 126 GB. SO D: 16 GB.	
Servidor Web Canales	node	Windows Server 2019 Standard o Datacenter x64. Nombre físico. IP LAN. IP Pública. Windows Server 2019 Standard or Datacenter x64. RAM 8 GB. CPU 64 Bits. 4 Cores de 2 Ghz. Discos SO C: 126 GB. SO D: 16 GB.	
www pgn com	technology-interface		

Diagrama de Arquitectura de la Solución Propuesta: motivadores del negocio

Migracion.1a.b.SIU Módulos



Imagen 4: Diagram: Migracion.1a.b.SIU Módulos

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

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

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

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

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

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

Requerimientos Asociados a los Submódulos

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

Catálogo de Elementos

Name	Type	Description	Properties
cc:Administración	application-collaboration		

Name	Type	Description	Properties
cc:Almacenamiento	application-collaboration	Espacio de almacenamiento operativo y transaccional de un módulo central del SUI migrado.	
cc:PGN SUI (módulo central)	application-collaboration	Módulo central SUI migrado. Módulo independiente y asignado a un dominio 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 redund 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.	

Riesgos.1. Migración funcional



Imagen 5: 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

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.	

Name	Type	Description	Properties
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 registrarán 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 incluidas en contrato 078, Migración Funcional SIU en atención al numeral 5.6 del anexo técnico del proyecto.	5.6 MIGRACIÓN DE DATOS
RSG2. Motor de búsqueda compartido	constraint	Establecer desde el principio el motor de búsqueda de contenidos compartido para los módulos del SUI migrados.	
RSG3. Estrategia como BI	constraint	Definir la arquitectura de Estrategia 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 contenidos compartido para los módulos del SUI migrados.	
RSG6. Componentes de negocio	constraint	Incluir el esfuerzo de creación de componentes estructurales y comunes a los módulos del SUI migrado requeridos por la arquitectura de referencia SUI. Algunos componentes requeridos son: * Administración de autorizaciones (integrado con el directorio PGN) * Motor de flujos de trabajo para diseño y organización del trabajo (Conciliación) * Componente de ruteo de documentos (Relatoría)	
RSG7. Asignación de roles y permisos de Acceso	constraint	RSG7. Asignación de roles y permisos de Acceso Los riesgos de autenticación como el Single Sign On (SSO), permite que si las credenciales de usuario se ven comprometidas, pueden dar permiso a un atacante acceder a todos o la mayoría de recursos y aplicaciones en la red. Se ha propuesto controlar los accesos a partir de la documentación que identifica la metodología de clasificación y gestión de usuarios roles y procesos de autenticación, a partir del control de acceso basado en roles RBAC (Identidades y autenticación), que permite tener una reacción más oportuna para controlar los accesos a diferentes módulos de los diferentes sistemas de Información. Los inicios de sesión de los usuarios asociados a cuenta de dominio de Active Directory deben tener en cuenta la asignación de roles de ingreso al servidor o roles de ingreso al motor de bases de datos. Las cuentas de usuario no deben ser creadas de administrador local (administrador), es una puerta de entrada para los ataques de fuerza bruta.	
RSG8. Intentos de accesos no autorizados	constraint	RSG8. Intentos de accesos no autorizados Los intentos no autorizados son una de las técnicas más comunes utilizadas en la actualidad, los diferentes tipos de amenazas de intrusiones SQL Injections, Denegaciones de Servicios, riesgos de Ransomware, Ingeniería social, malware y otras amenazas, permite que se proponga implementación de soluciones de Seguridad perimetral a partir de la implementación de WAF para controlar las peticiones externas y evaluación de vulnerabilidades y escaneo para conocer puertos abiertos y establecer medidas.	

Name	Type	Description	Properties
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 Always 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

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

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

versión 0.5

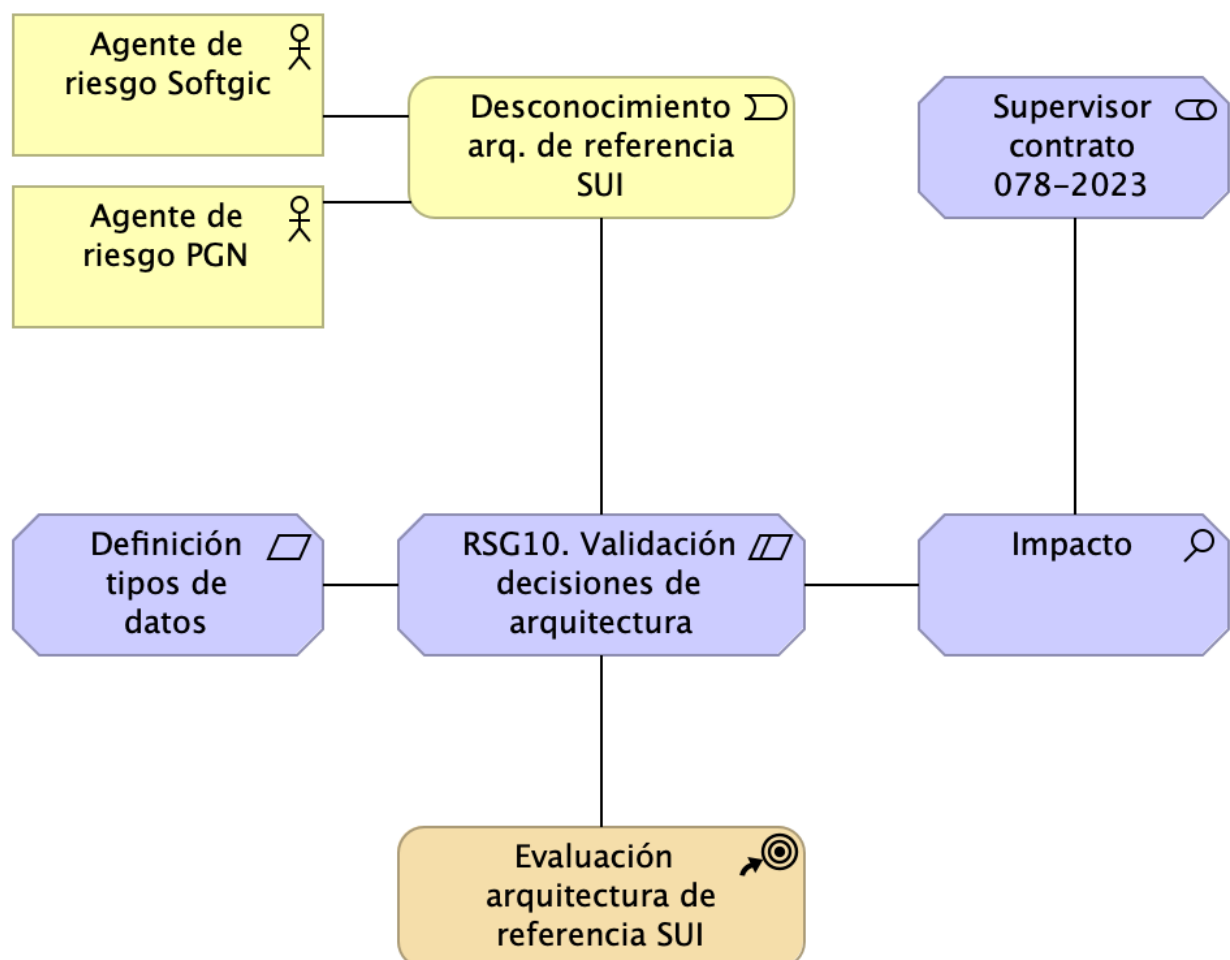


Imagen 6: Diagram: Riesgos.2. Modelo Riesgo RSG10

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		

Riesgos.3. Modelo Riesgo RSG11

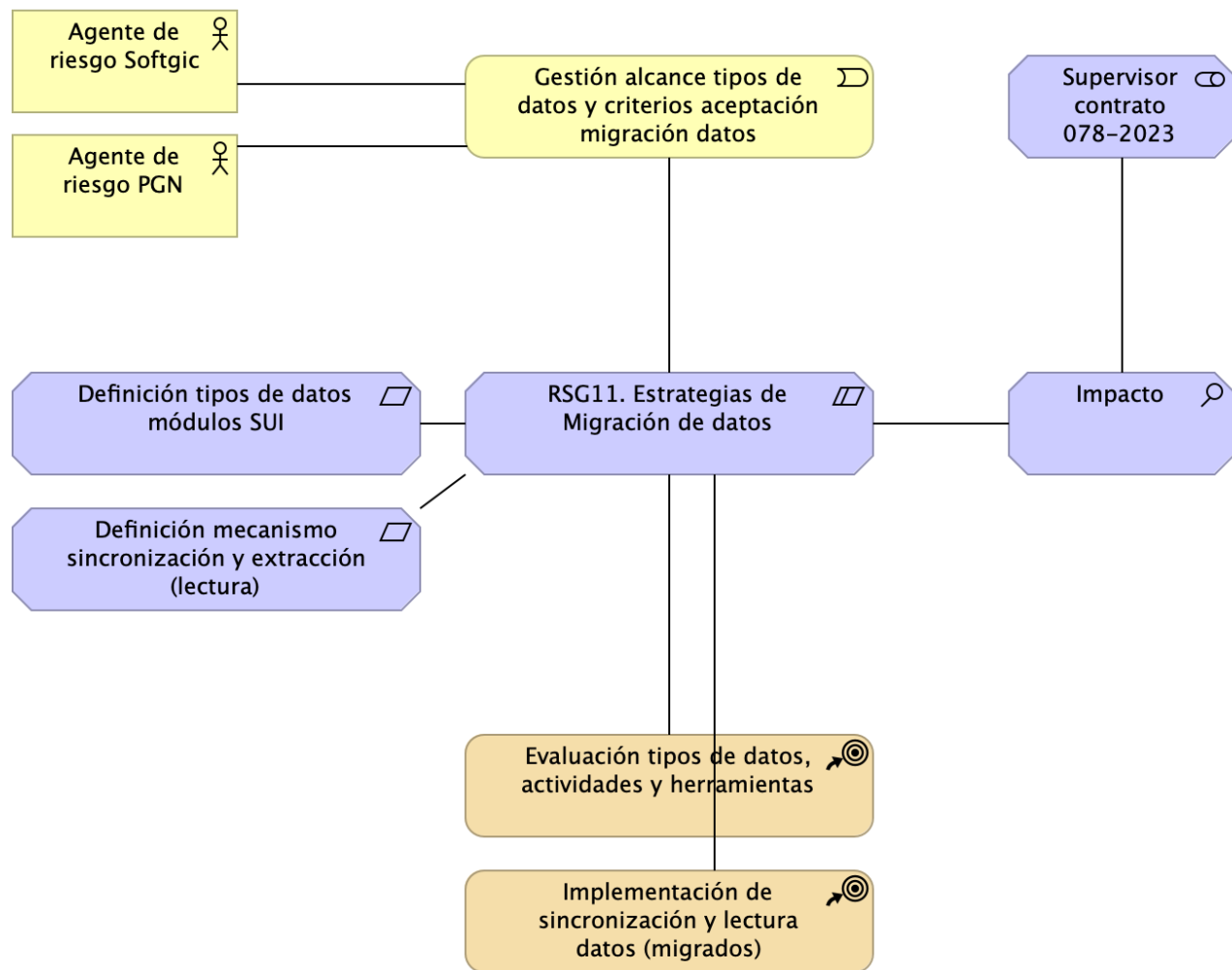


Imagen 7: Diagram: Riesgos.3. Modelo Riesgo RSG11

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 5: 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	Sobretabajo del proyecto 078, esfuerzo y presupuesto.	
Agente de riesgo PGN	business-actor	Arquitecto PGN	
Agente de riesgo Softgic	business-actor	Arquitecto Softgic	

Name	Type	Description	Properties
Gestión alcance tipos de datos y criterios aceptación migración datos	business-event		
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
Evaluación tipos de datos, actividades y herramientas	course-of-action	La frecuencia del proceso de evaluación de la arquitectura es eventual, mínimo una vez cada dos semanas.	
Implementación de sincronización y lectura datos (migrados)	course-of-action	La frecuencia del proceso de evaluación de la arquitectura es eventual, mínimo una vez cada dos semanas.	
Definición mecanismo sincronización y extracción (lectura)	requirement		
Definición tipos de datos módulos SUI	requirement		
Supervisor contrato 078-2023	stakeholder		

Diagrama de Arquitectura de la Solución Propuesta: interoperabilidad

Migracion.1c.SIU Modulos Colaboración



Imagen 8: 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 estandar descrito en el diagrama.

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

Catálogo de Elementos

Name	Type	Description	Properties
cc:Almacenamiento	application-collaboration	Espacio de almacenamiento operativo y transaccional de un módulo central del SUI migrado.	
cc:PGN SUI (módulo central)	application-collaboration	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN.	
cc:PGN SUI (módulo central)	application-collaboration	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN.	

Name	Type	Description	Properties
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. Centralización de la comunicación con otros módulos del SUI migrado.	
API SUI	application-interface	API de representación del módulo. Centralización de la comunicación con otros módulos del SUI migrado.	
API SUI 2	application-interface	API de representación del módulo. Centralización de la comunicación con otros módulos del SUI migrado.	

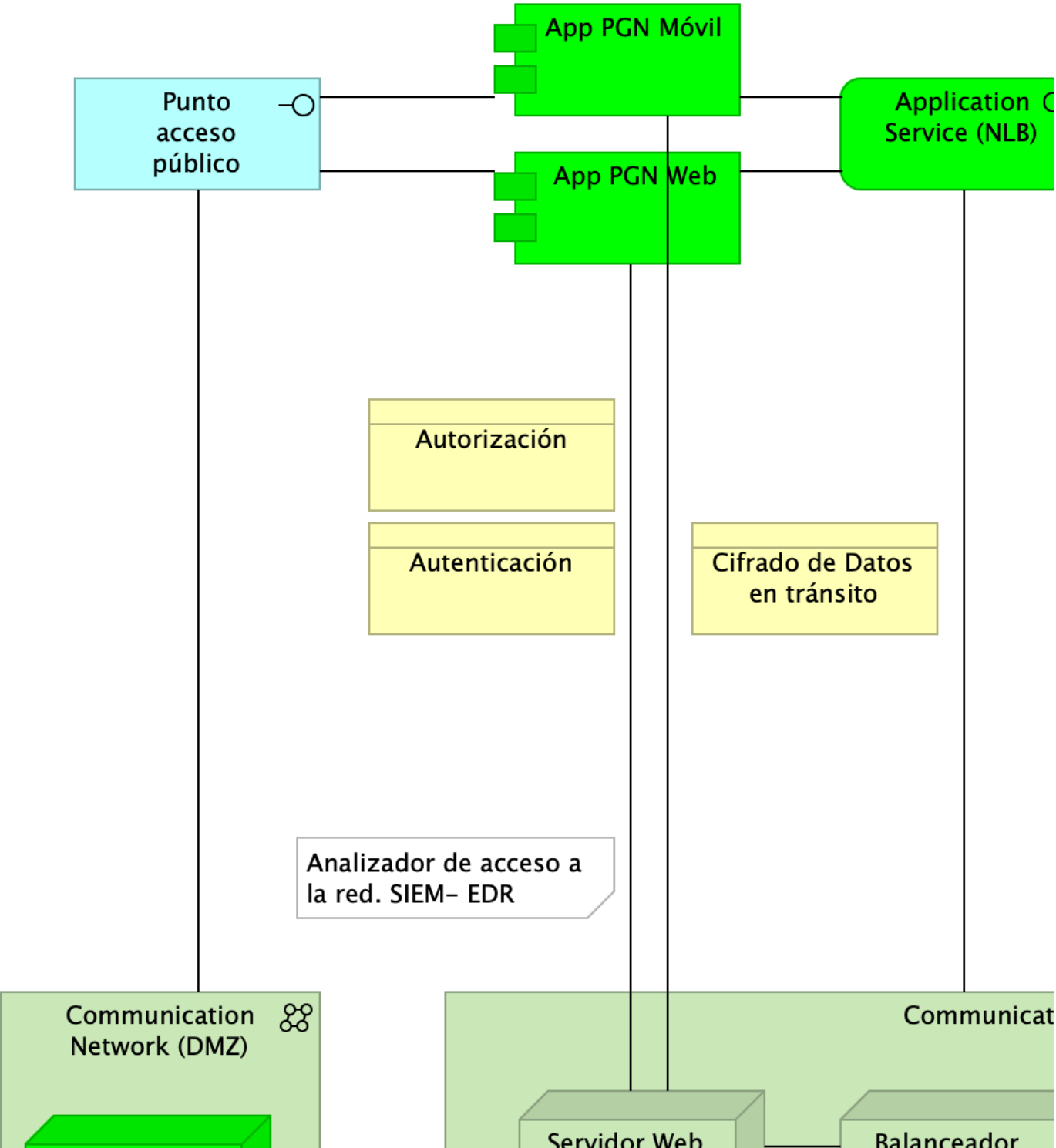
Diagrama de Arquitectura de la Solución Propuesta: gestión de autenticación,

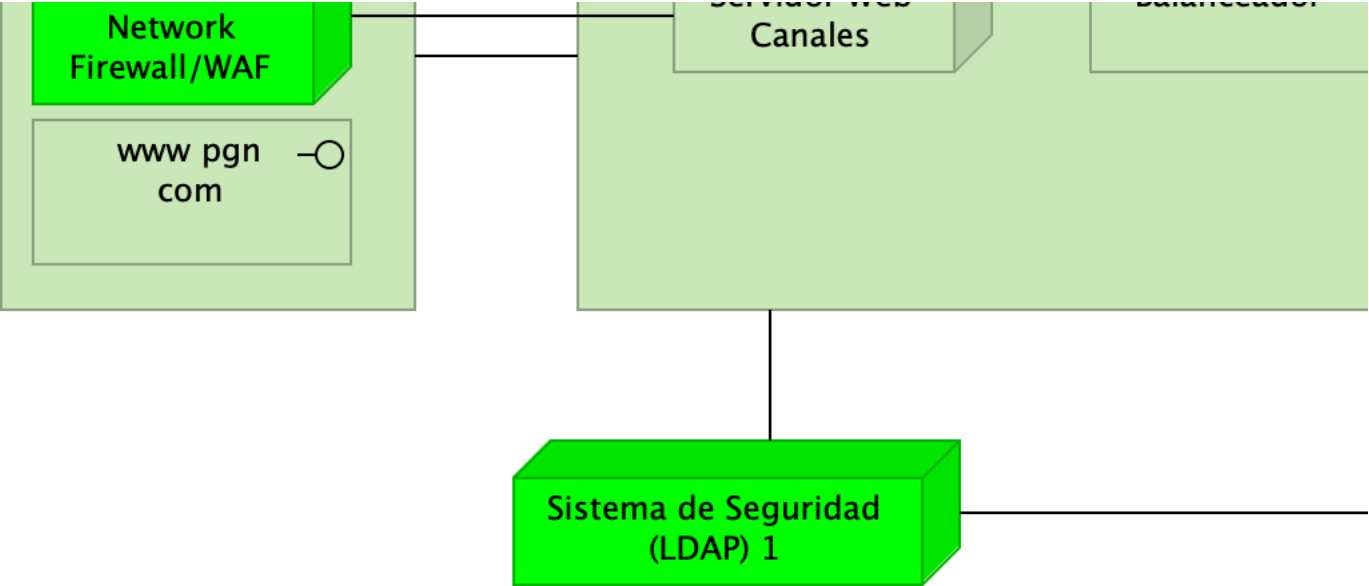
usuarios y roles ## Seguridad.2. Lineabase.0.SIU Aplicación

PGN. Migración Sistemas Misionales. Fase 2.

Submódulos Sistema Único de Información.
Requerimientos físicos y software base
asociados a módulos SUI migrado.

versión 0.2.2





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

Name	Type	Description	Properties
App PGN Móvil	application-component	<p>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.</p> <p>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.</p> <p>La informacion contenida en las bases de datos debe tener los mecanismos de cifrado que en otros apartados se han mencionado.</p> <p>La legislación que hay que tener como referencia, ley 1581 de 2012. Decreto 1377 de 2013</p> <p>La metodologia empleada tendrá las siguientes fases:</p> <ul style="list-style-type: none">• FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como: o Recopilación de dominios/IPs/puertos/servicios o Recopilación de metadatos o Uso de Google Dorks.• ANÁLISIS DE VULNERABILIDADES: Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.• EXPLOTACIÓN:<ul style="list-style-type: none">• Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo: o Inyección de código o Inclusión de ficheros locales o remotos o Evasión de autenticación o Carencia de controles de autorización o Ejecución de comandos en el lado del servidor o Ataques tipo Cross Site Request Forgery o Control de errores o Gestión de sesiones o Fugas de información o Secuestros de sesión o Comprobación de las condiciones para realizar una denegación de servicio.• POST EXPLOTACIÓN: En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adiciones con el objetivo de comprobar la criticidad de esta. <p>No URL IP 1. https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz 135.181.185.207</p>	<p><i>plantilla: element-md-bold</i> <i>brecha: 100</i></p>

Name	Type	Description	Properties
App PGN Web	application-component	<p>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 Ethical Hacking.</p> <p>Los resultados permitirán identificar los requisitos de seguridad que los sistemas de informacion o servicios web deberán cumplir.</p> <p>La metodologia empleada tendrá las siguientes fases:</p> <ul style="list-style-type: none"> • FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como: o Recopilación de dominios/IPs/puertos/servicios o Recopilación de metadatos o Uso de Google Dorks. • ANÁLISIS DE VULNERABILIDADES: Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades. • EXPLOTACIÓN: • Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo: o Inyección de código o Inclusión de ficheros locales o remotos o Evasión de autenticación o Carencia de controles de autorización o Ejecución de comandos en el lado del servidor o Ataques tipo Cross Site Request Forgery o Control de errores o Gestión de sesiones o Fugas de información o Secuestros de sesión o Comprobación de las condiciones para realizar una denegación de servicio. • POST EXPLOTACIÓN: En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adiciones con el objetivo de comprobar la criticidad de esta. No URL IP 1. https://runtime-test.lappiz.io/#/auth/login/PGN_Lappiz 135.181.185.207 El Login deberá evidenciar el control de errores, al momento de realizar la validación deberá mensaje de error para el caso que se autentique con credenciales erradas. 	<p>plataforma: angular 11 brecha: 100</p>
Config	application-component		plataforma: cs
Punto acceso público	application-interface	URL tipo C HTTP	
Application Service (NLB)	application-service		plataforma: angular 11 brecha: 100
Interfaz de datos 1	application-service		
Interfaz de datos 2	application-service		

Name	Type	Description	Properties
Autenticación	business-object	<p>Con el objetivo de incrementar el nivel de seguridad, para el proceso de autenticación se tendrán en cuenta las siguientes consideraciones:</p> <p>Validación del proceso de gestión de usuarios: La fortaleza de la autenticación dependerá del proceso de gestión de usuarios implementado por parte de la entidad. Se debe tener en cuenta los lineamientos definidos en la política Específica de Control de Acceso.</p> <p>Autenticación con integración de Windows: La autenticación permitirá que los usuarios asignados al dominio, una vez que se ingresen las credenciales, y realizada la validación, se autorizará el acceso a los servicios y/o soluciones a partir de la integración del directorio activo con la integración del LDAP – (Lightweight Directory Access Protocol).</p> <p>Los tipos de autenticación realizadas a partir de las identidades administradas de los recursos de Azure, entidades de Servicio y Certificados, podrán ser integrado con los dominios del directorio activo (DA) local. Por lo que respecta a la autenticación, será generado con la asignación de usuarios y credenciales definidas alineadas con la política Específica de Control de Acceso., a partir de la integración será validado el ingreso a las diferentes soluciones y/o sistemas de información de la PGN.</p> <p>Manejo y uso de contraseñas: Los servidores públicos deberán tener en cuenta los lineamientos definidos para la creación y gestión de contraseñas del Sistema de Gestión de Seguridad de la Información SGSI de la Procuraduría General de la Nación.</p> <p>Utilización de canales cifrados: El proceso de autenticación tendrá mecanismos de transmisión seguro. El uso del TLS (Transport Layer Security), será necesario para el acceso a la página de autenticación que ayude a garantizar la autenticidad de la aplicación a los funcionarios, como en la transmisión de las credenciales.</p> <p>Bloqueo de cuentas: Aquellas cuentas sobre las que se han realizados múltiples intentos de conexiones fallidas, cinco (5) intentos erróneos, se tendrá implementado un bloqueo temporal o permanente como mecanismo de seguridad para evitar amenazas de ataques.</p>	
Autorización	business-object	<p>Metodología</p> <p>Los mecanismos de autorización para el acceso a los sistemas de información de la procuraduría general de la nación describen la forma de cómo se restringe el acceso a los diferentes módulos (Misionales (SIM), Registros de Inhabilidades (SIRI), Nómina, Control Interno y relatoría, entre otros.), y que se considera un mecanismo de protección, que ayuda a reaccionar ante cualquier operación no autorizada. El control de acceso basado en roles (RBAC), enfoca la idea de que a los funcionarios se les otorgue los permisos de acceso a los recursos, basados en los roles y/o perfiles que este posee. Este control posee dos características fundamentales: i) los accesos son controlados por medio de los roles y/o perfiles asignados, quiere decir, a los servidores públicos, contratistas, terceros y otros colaboradores autorizados para interactuar con los sistemas de información se le asignan los roles y el encargado/responsable definirá los permisos, que a su vez están relacionados con los roles, ii) Los roles pueden ser definidos a nivel jerárquico, es decir que un rol podrá ser miembro de otro rol.</p> <p>Un proceso de autorización basado en roles, identifica tres factores importantes, i) Todos los servidores públicos, contratistas, terceros y otros Colaboradores, deben tener un rol asignado, si no es asignado no podrá realizar ninguna acción relacionada con el acceso, ii) un usuario podrá hacer uso de</p>	

Name	Type	Description	Properties
		<p>los permisos asociados a los roles asignados, el cual deberá realizar el inicio de sesión el usuario asignado del Directorio activo (DA), iii) los servidores públicos, contratistas, terceros y otros, solo podrán realizar acciones para las cuales han sido autorizados por medio de la activación de sus roles y/o perfiles.</p> <p>EL control definido para los accesos basados en roles RBAC, permitirá que solo las personas autorizadas de la PGN podrán acceder a ciertos recursos (programas, equipos, aplicaciones, bases de datos, etc.) definido por sus funciones laborales, lo que permitirá controlar los accesos desde diferentes escenarios: Sistemas de información, redes y aplicaciones.</p> <p>Gestión de identidades y Control de acceso:</p> <p>Gestor de identidades: En esta gestión se planifica el ciclo de vida de las identidades de usuario y se realizan los procesos de sincronización, de acuerdo a los suministros de accesos establecidos por la entidad, los cuales son integrados con el servidor que gestiona la identidad y control de acceso.</p> <p>Gestor de roles: La asignación de roles es sincronizada con la identidad de usuario en el servidor de dominio. Para esta gestión se crean las reglas y condiciones que determinan si un usuario puede o no pertenecer a un rol definido por la entidad.</p> <p>Para el gobierno y gestión de identidades y de acceso, se identificó como primera medida la implementación de la siguiente metodología.</p> <p>REGLAS PARA LA CREACIÓN DE USUARIOS.</p> <p>Identificación de Mecanismos:</p> <p>En este ítem se deben identificar las herramientas con las que cuenta la entidad, las cuales deberán ser registradas en el documento denominado: "Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_1 (Mecanismos)".</p> <p>Identificación de Roles y Privilegios</p> <p>Este ítem proporciona al sistema la definición de las políticas organizacionales en cuanto a la definición de los privilegios y roles de los diferentes actores en cada uno de los aplicativos con los que estos interactúan dentro de sus funciones, registradas en el documento denominado: "Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_2 (Roles)".</p> <p>Aprovisionamiento de cuentas</p> <p>Este ítem establece el proceso adecuado para el aprovisionamiento y desaprovisionamiento de cuentas de usuarios en las diferentes aplicaciones, permitiendo toda la gestión de ellas por medio de un sistema de directorio único y centralizado, Este aprovisionamiento se encuentra registrado en el documento denominado: "Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_4 y Hoja_5 (Permisos)".</p> <p>Establecimiento de mecanismos de control de acceso:</p> <p>Este ítem controla que usuarios tienen permitido el acceso a los diferentes aplicativos o herramientas dentro de la organización permitiendo segregar las funciones dependiendo del rol del usuario en cada sistema, Este establecimiento se encuentra registrado en el documento denominado: "Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_3 (Acceso)".</p> <p>Definición de Privilegios y accesos.</p> <p>Los accesos y privilegios serán identificados en la matriz, encargado identificar cada uno de los roles y perfiles que se tendrá cada usuario hacia los sistemas de información cumpliendo con el principio del menor privilegio, teniendo en cuenta que los usuarios deberán tener exclusivamente los permisos y privilegios que necesita para el desarrollo de sus actividades. La matriz identificará i) los roles que se deben crear para cada sistema de información, ii) los privilegios que requiere cada rol del sistema y iii) los</p>	

Name	Type	Description	Properties
		<p>niveles de accesos requeridos, (Consultar, Modificar, Eliminar) (CRUD) y iv) Tipos de usuarios, roles que pueden ser asignados al perfil, entre otros.</p> <p>Configuración de permisos</p> <p>La configuración con de los perfiles con sus accesos y privilegios en los sistemas de información se debe realizar empleando las herramientas propias de la procuraduría general de la nacional PGN, y serán asignados los permisos según la matriz de roles y permisos.</p> <p>Identificación de Mecanismos:</p> <p>En este ítem se deben identificar las herramientas con las que cuenta la entidad, las cuales deberán ser registradas en el documento denominado:</p> <p>“Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_1 (Mecanismos)”.</p> <p>Identificación de Roles y Privilegios</p> <p>Este ítem proporciona al sistema la definición de las políticas organizacionales en cuanto a la definición de los privilegios y roles de los diferentes actores en cada uno de los aplicativos con los que estos interactúan dentro de sus funciones, registradas en el documento denominado:</p> <p>“Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_2 (Roles)”.</p> <p>Aprovisionamiento de cuentas</p> <p>Este ítem establece el proceso adecuado para el aprovisionamiento y des aprovisionamiento de cuentas de usuarios en las diferentes aplicaciones, permitiendo toda la gestión de ellas por medio de un sistema de directorio único y centralizado, Este aprovisionamiento se encuentra registrado en el documento denominado:</p> <p>“Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_4 y Hoja_5 (Permisos)”.</p> <p>Establecimiento de mecanismos de control de acceso:</p> <p>Este ítem controla que usuarios tienen permitido el acceso a los diferentes aplicativos o herramientas dentro de la organización permitiendo segregar las funciones dependiendo del rol del usuario en cada sistema, Este establecimiento se encuentra registrado en el documento denominado: “Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_3 (Acceso)”.</p> <p>Definición de Privilegios y accesos.</p> <p>Los accesos y privilegios serán identificados en la matriz, encargado identificar cada uno de los roles y perfiles que se tendrá cada usuario hacia los sistemas de información cumpliendo con el principio del menor privilegio, teniendo en cuenta que los usuarios deberán tener exclusivamente los permisos y privilegios que necesita para el desarrollo de sus actividades. La matriz identificará i) los roles que se deben crear para cada sistema de información, ii) los privilegios que requiere cada rol del sistema y iii) los niveles de accesos requeridos, (Consultar, Modificar, Eliminar) (CRUD) y iv) Tipos de usuarios, roles que pueden ser asignados al perfil, entre otros.</p> <p>Configuración de permisos</p> <p>La configuración con de los perfiles con sus accesos y privilegios en los sistemas de información se debe realizar empleando las herramientas propias de la procuraduría general de la nacional PGN, y serán asignados los permisos según la matriz de roles y permisos.</p>	

Name	Type	Description	Properties
Cifrado de Datos en tránsito	business-object	<p>Proteger la información propia de la PGN utilizando mecanismos de cifrado que permita garantizar los pilares de Seguridad de la Información Confidencialidad e integridad, asimismo reducir los riesgos de la información mediante la ayuda de Técnicas Criptograficas.</p> <p>Como mecanismos se propone implementar estos mecanismos de cifrado, como el protocolo TLS (Transport Layer Security) que permite a dos partes identificarse y autenticarse entre sí y comunicarse con confidencialidad e integridad de datos a partir de la conexión del usuario y un servidor WEB.</p> <p>Se propone integrar certificados SSL, que permite cifrar la información confidencial a fin de que solo los autorizados puedan tener acceso a ella, y así evitar manipulación de información confidencial.</p> <p>La Seguridad que brinda SSL, da garantía para acceder a los aplicativos de PNG.</p> <p>Como implementar certificados SSL?</p> <p>Podrán ser adquiridos a través del proveedor de dominios.</p> <p>TLS el protocolo que surge para reforzar la seguridad de los certificados SSL, que funciona como mecanismo de encriptación para que sea realmente transparente el envío de la información, proporcionando una autenticación solida, restringiendo la manipulación, interceptación y alteración de mensajes.</p> <p>La ultima versión del TLS es la 1.3</p>	
Cifrado de datos en tránsito	business-object	<p>Proteger la información propia de la PGN utilizando mecanismos de cifrado que permita garantizar los pilares de Seguridad de la Información Confidencialidad e integridad, asimismo reducir los riesgos de la información mediante la ayuda de Técnicas Criptograficas.</p> <p>Como mecanismos se propone implementar estos mecanismos de cifrado, como el protocolo TLS (Transport Layer Security) que permite a dos partes identificarse y autenticarse entre sí y comunicarse con confidencialidad e integridad de datos a partir de la conexión del usuario y un servidor WEB.</p> <p>Se propone integrar certificados SSL, que permite cifrar la información confidencial a fin de que solo los autorizados puedan tener acceso a ella, y así evitar manipulación de información confidencial.</p> <p>La Seguridad que brinda SSL, da garantía para acceder a los aplicativos de PNG.</p> <p>Como implementar certificados SSL?</p> <p>Podrán ser adquiridos a través del proveedor de dominios.</p> <p>TLS el protocolo que surge para reforzar la seguridad de los certificados SSL, que funciona como mecanismo de encriptación para que sea realmente transparente el envío de la información, proporcionando una autenticación solida, restringiendo la manipulación, interceptación y alteración de mensajes.</p> <p>La ultima versión del TLS es la 1.3</p>	
Communication Network (DMZ)	communication-network		
Communication Network (LAN)	communication-network		
Communication Network (internet)	communication-network		
Balanceador	node		
Firewall BDD	node		<i>brecha:</i> 100
Network Firewall/WAF	node		<i>brecha:</i> 100
Servidor BDD App	node	<p>Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB.</p> <p>CPU 64 Bits, 4 Cores > 2 Ghz</p> <p>Discos SO C: 126 GB, Backup E: 511 GB, SQL Data F: 510 GB, SQL Log G: 510 GB, TempDB G: 63.6 GB.</p>	
Servidor BDD Config	node	<p>Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB.</p> <p>CPU 64 Bits, 4 Cores > 2 Ghz</p> <p>Discos SO C: 80 GB, Backup E: 250 GB, SQL Data F: 250 GB, SQL Log G: 250 GB, TempDB G: 30 GB.</p>	

Name	Type	Description	Properties
Servidor Web App	node	Windows Server 2019 Standard o Datacenter x64. Nombre físico. IP LAN. IP Pública. Windows Server 2019 Standard or Datacenter x64. RAM 8 GB. CPU 64 Bits. 4 Cores de 2 Ghz. Discos SO C: 126 GB. SO D: 16 GB.	
Servidor Web Canales	node	Windows Server 2019 Standard o Datacenter x64. Nombre físico. IP LAN. IP Pública. Windows Server 2019 Standard or Datacenter x64. RAM 8 GB. CPU 64 Bits. 4 Cores de 2 Ghz. Discos SO C: 126 GB. SO D: 16 GB.	
Sistema de Seguridad (LDAP) 1	node	Sistema de Seguridad (LDAP) 1. Control de acceso internet, La autenticación podrá estar integrada con el directorio activo, a partir de la generación de código para el ingreso con 2FA, que podrá generar un código la plataforma de correo corporativo, el cual solicitará el código de autenticación y una vez ingresado podrá redirigir al sitio.	<i>brecha: 100</i>
Sistema de Seguridad (LDAP) 2	node	Sistema de Seguridad (LDAP) 2. Control de acceso internet, La solución se podrá integrar con el directorio activo, a partir de la generación del 2FA, que podrá generar un código por desde la plataforma de office 365, el cual solicitará el código de autenticación y una vez ingresado podrá acceder al sitio.	<i>brecha: 100</i>
www.pgn.com	technology-interface		

Diagrama de Clases y Componentes de solución

Migracion.1b.1. SIU Módulos Componentes

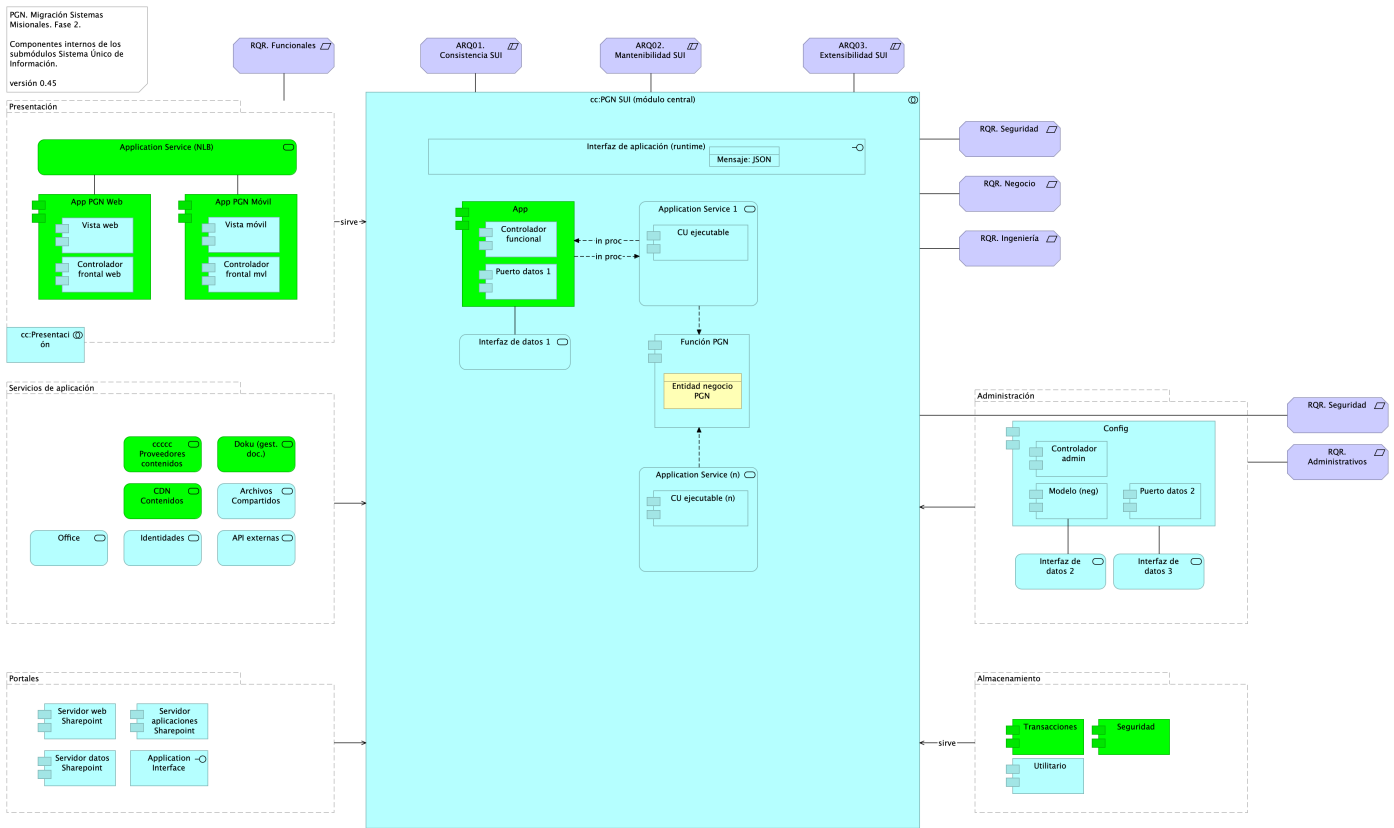


Imagen 9: Diagram: Migracion.1b.1. SIU Módulos Componentes

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 constituidos por submódulos dispuestos en relación de utilitarios (que sirven) a los componentes misionales del SUI, ubicados en el centro en la diagrama.

La organización de componentes de migración SUI facilita focalizar la selección de tecnogeias. 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

Name	Type	Description	Properties
App PGN Móvil	application-component	<p>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.</p> <p>Protección de datos personales,</p> <p>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.</p> <p>La informacion contenida en las bases de datos debe tener los mecanismos de cifrado que en otros apartados se han mencionado.</p> <p>La legislación que hay que tener como referencia, ley 1581 de 2012. Decreto 1377 de 2013</p> <p>La metodologia empleada tendrá las siguientes fases:</p> <ul style="list-style-type: none">• FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como: o Recopilación de dominios/IPs/puertos/servicios o Recopilación de metadatos o Uso de Google Dorks.• ANÁLISIS DE VULNERABILIDADES: Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.• EXPLOTACIÓN:<ul style="list-style-type: none">• Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo: o Inyección de código o Inclusión de ficheros locales o remotos o Evasión de autenticación o Carencia de controles de autorización o Ejecución de comandos en el lado del servidor o Ataques tipo Cross Site Request Forgery o Control de errores o Gestión de sesiones o Fugas de información o Secuestros de sesión o Comprobación de las condiciones para realizar una denegación de servicio.• POST EXPLOTACIÓN: En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adiciones con el objetivo de comprobar la criticidad de esta. <p>No URL IP 1. https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz 135.181.185.207</p>	<p><i>plantilla: element-md-bold</i> <i>brecha: 100</i></p>

Name	Type	Description	Properties
App PGN Web	application-component	<p>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 Ethical Hacking.</p> <p>Los resultados permitirán identificar los requisitos de seguridad que los sistemas de informacion o servicios web deberán cumplir.</p> <p>La metodologia empleada tendrá las siguientes fases:</p> <ul style="list-style-type: none"> • FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como: o Recopilación de dominios/IPs/puertos/servicios o Recopilación de metadatos o Uso de Google Dorks. • ANÁLISIS DE VULNERABILIDADES: Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades. • EXPLOTACIÓN: • Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo: o Inyección de código o Inclusión de ficheros locales o remotos o Evasión de autenticación o Carencia de controles de autorización o Ejecución de comandos en el lado del servidor o Ataques tipo Cross Site Request Forgery o Control de errores o Gestión de sesiones o Fugas de información o Secuestros de sesión o Comprobación de las condiciones para realizar una denegación de servicio. • POST EXPLOTACIÓN: En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adiciones con el objetivo de comprobar la criticidad de esta. No URL IP 1. https://runtimeptest.lappiz.io/#/auth/login/ PGN_Lappiz 135.181.185.207 El Login deberá evidenciar el control de errores, al momento de realizar la validación deberá mensaje de error para el caso que se autentique con credenciales erradas. 	<p>plataforma: angular 11 brecha: 100</p>
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	<p>- Verificados los SSL, se recomienda adquirir SSL seguros, con entidades certificadoras.</p> <p>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.</p>	plataforma: js
Controlador funcional	application-component		plataforma: js
Función PGN	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

Name	Type	Description	Properties
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	<p>- Verificados los SSL, se recomienda adquirir SSL seguros, con entidades certificadoras.</p> <p>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.</p> <p>4. SERVICIOS IDENTIFICADOS:</p> <p>Servidor web: Microsoft-IIS/10.0</p> <p>Marco de Programación: ASP.NET</p> <p>Huellas digitales identificadas:</p> <p>Huella digital SHA-256</p> <p>"FC:79:06:7E:F5:24:20:50:F1:C0:74:F7:85:56:B9:05:B7:33:A3:2D:44:A0:48"</p> <p>Huella digital SHA1</p> <p>"8C:48:BD:E2:F5:18:18:C3:85:96:68:44:2E:28:A0:68:08:2F:0A:BE"</p>	plataforma: html
Application Interface	application-interface		
Interfaz de aplicación (runtime)	application-interface	<p>Servidor web: Microsoft-IIS/10.0</p> <p>Marco de Programación: ASP.NET</p> <p>Huellas digitales identificadas:</p> <p>Huella digital SHA-256</p> <p>"FC:79:06:7E:F5:24:20:50:F1:C0:74:F7:85:56:B9:05:B7:33:A3:2D:44:A0:48"</p> <p>Huella digital SHA1</p> <p>"8C:48:BD:E2:F5:18:18:C3:85:96:68:44:2E:28:A0:68:08:2F:0A:BE"</p>	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	business-object	Represnta un objeto de negocio del contexto de la entidad PGN,, por ejemplo: un decreto, una intervención, una conciliación.	

Name	Type	Description	Properties
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 redundante 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

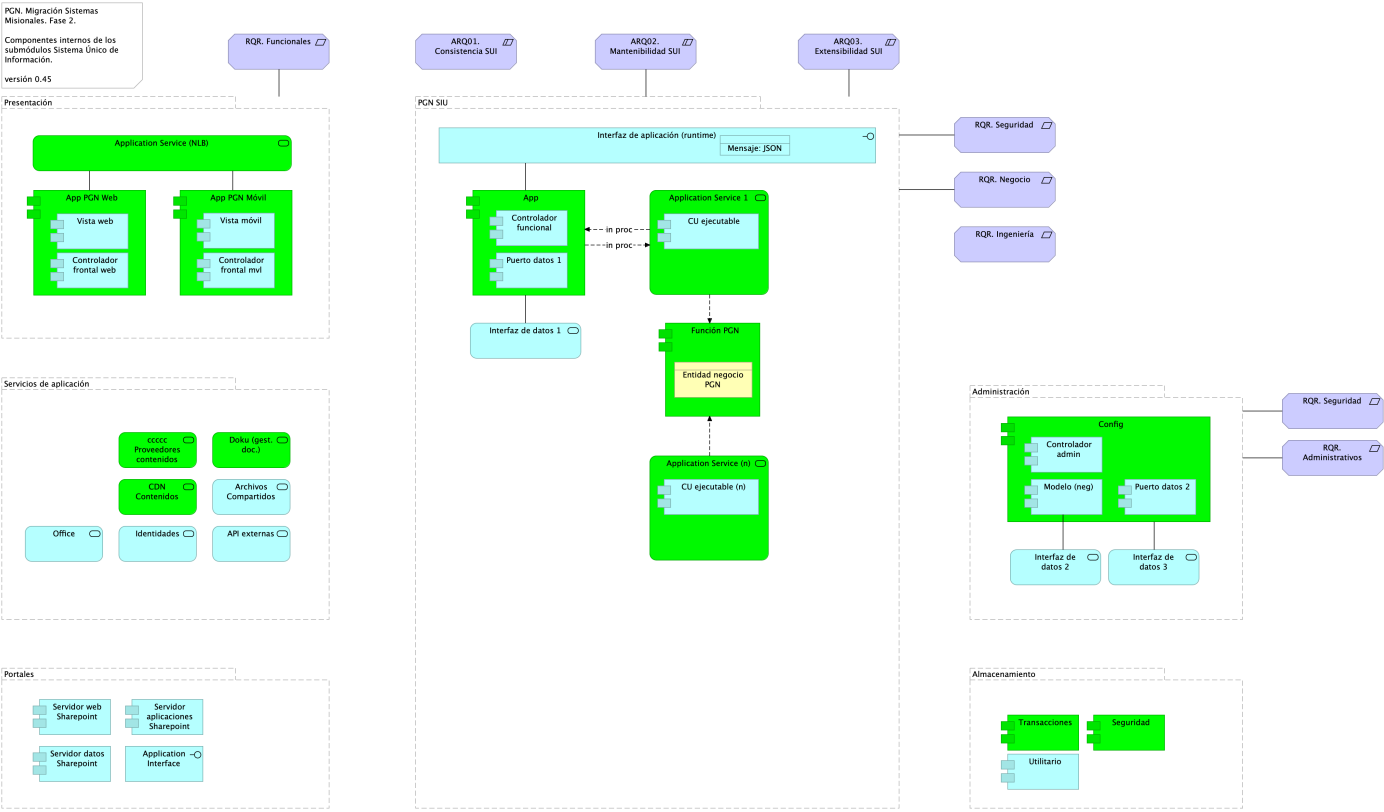


Imagen 10: Diagram: Migracion.1b.2. SIU Módulos Componentes. Brecha

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

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

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

Catálogo de Elementos

Name	Type	Description	Properties
App	application-component		plataforma: node Js brecha: 100

Name	Type	Description	Properties
App PGN Móvil	application-component	<p>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.</p> <p>Protección de datos personales,</p> <p>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.</p> <p>La informacion contenida en las bases de datos debe tener los mecanismos de cifrado que en otros apartados se han mencionado.</p> <p>La legislación que hay que tener como referencia, ley 1581 de 2012. Decreto 1377 de 2013</p> <p>La metodologia empleada tendrá las siguientes fases:</p> <ul style="list-style-type: none">• FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como: o Recopilación de dominios/IPs/puertos/servicios o Recopilación de metadatos o Uso de Google Dorks.• ANÁLISIS DE VULNERABILIDADES: Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.• EXPLOTACIÓN: <ul style="list-style-type: none">• Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo: o Inyección de código o Inclusión de ficheros locales o remotos o Evasión de autenticación o Carencia de controles de autorización o Ejecución de comandos en el lado del servidor o Ataques tipo Cross Site Request Forgery o Control de errores o Gestión de sesiones o Fugas de información o Secuestros de sesión o Comprobación de las condiciones para realizar una denegación de servicio.• POST EXPLOTACIÓN: En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adiciones con el objetivo de comprobar la criticidad de esta. <p>No URL IP 1. https://runtimetest.lappiz.io/#!/auth/login/PGN_Lappiz 135.181.185.207</p>	<p><i>plantilla: element-md-bold</i> <i>brecha: 100</i></p>

Name	Type	Description	Properties
App PGN Web	application-component	<p>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 Ethical Hacking.</p> <p>Los resultados permitirán identificar los requisitos de seguridad que los sistemas de informacion o servicios web deberán cumplir.</p> <p>La metodologia empleada tendrá las siguientes fases:</p> <ul style="list-style-type: none"> • FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como: o Recopilación de dominios/IPs/puertos/servicios o Recopilación de metadatos o Uso de Google Dorks. • ANÁLISIS DE VULNERABILIDADES: Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades. • EXPLOTACIÓN: • Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo: o Inyección de código o Inclusión de ficheros locales o remotos o Evasión de autenticación o Carencia de controles de autorización o Ejecución de comandos en el lado del servidor o Ataques tipo Cross Site Request Forgery o Control de errores o Gestión de sesiones o Fugas de información o Secuestros de sesión o Comprobación de las condiciones para realizar una denegación de servicio. • POST EXPLOTACIÓN: En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adiciones con el objetivo de comprobar la criticidad de esta. No URL IP 1. https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz 135.181.185.207 El Login deberá evidenciar el control de errores, al momento de realizar la validación deberá mensaje de error para el caso que se autentique con credenciales erradas. 	<p>plataforma: angular 11 brecha: 100</p>
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	<p>- Verificados los SSL, se recomienda adquirir SSL seguros, con entidades certificadoras.</p> <p>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.</p>	plataforma: js
Controlador funcional	application-component		plataforma: js
Función PGN	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

Name	Type	Description	Properties
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	<p>- Verificados los SSL, se recomienda adquirir SSL seguros, con entidades certificadoras.</p> <p>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.</p> <p>4. SERVICIOS IDENTIFICADOS:</p> <p>Servidor web: Microsoft-IIS/10.0</p> <p>Marco de Programación: ASP.NET</p> <p>Huellas digitales identificadas:</p> <p>Huella digital SHA-256</p> <p>"FC:79:06:7E:F5:24:20:50:F1:C0:74:F7:85:56:B9:05:B7:33:A3:2D:44:A0:48"</p> <p>Huella digital SHA1</p> <p>"8C:48:BD:E2:F5:18:18:C3:85:96:68:44:2E:28:A0:68:08:2F:0A:BE"</p>	plataforma: html
Application Interface	application-interface		
Interfaz de aplicación (runtime)	application-interface	<p>Servidor web: Microsoft-IIS/10.0</p> <p>Marco de Programación: ASP.NET</p> <p>Huellas digitales identificadas:</p> <p>Huella digital SHA-256</p> <p>"FC:79:06:7E:F5:24:20:50:F1:C0:74:F7:85:56:B9:05:B7:33:A3:2D:44:A0:48"</p> <p>Huella digital SHA1</p> <p>"8C:48:BD:E2:F5:18:18:C3:85:96:68:44:2E:28:A0:68:08:2F:0A:BE"</p>	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		
cccc Proveedores contenidos	application-service		brecha: 100
Entidad negocio PGN	business-object	Represnta un objeto de negocio del contexto de la entidad PGN,, por ejemplo: un decreto, una intervención, una conciliación.	

Name	Type	Description	Properties
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 redundante 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 conflicto entre ellos.	
Portales	grouping	Submódulo de portales internos de la PGN a donde llega el SUI. Interfaz web que usa al SUI para llegar a direcciones y subdirecciones de la PGN. La plataforma principal de portales en este contexto es Sharepoint de Microsoft.	
Presentación	grouping	Submódulo de presentación del SUI. interfaz gráfica, interfaz web visible a los usuarios clientes y funcionarios de la PGN.	
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.	

Diagrama de Arquitectura de Integración Continua, Devops y Despliegues de Capas

Migracion.4. CI

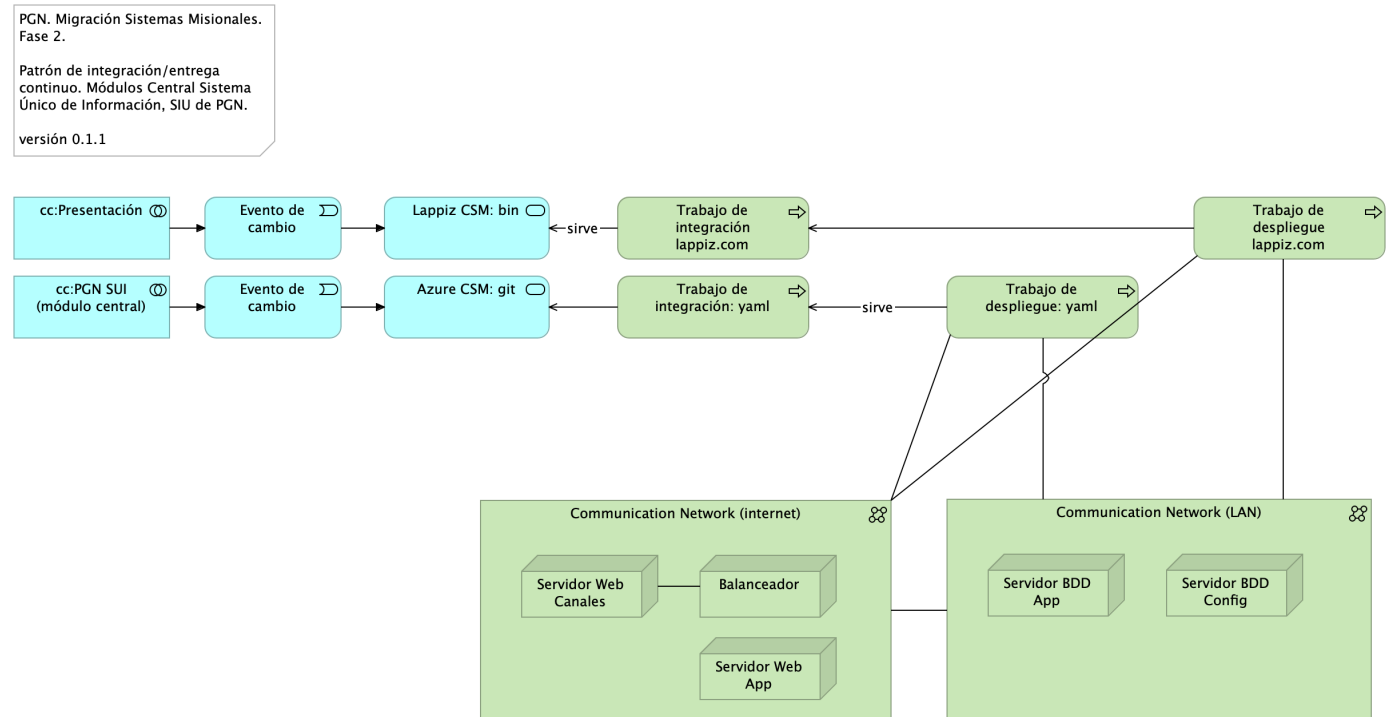


Imagen 11: Diagram: Migracion.4. CI

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

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

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

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.	
Evento de cambio	application-event		
Evento de cambio	application-event		
Azure CSM: git	application-service		
Lappiz CSM: bin	application-service		
Communication Network (LAN)	communication-network		
Communication Network (internet)	communication-network		
Balanceador	node		
Servidor BDD App	node	Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz Discos SO C: 126 GB, Backup E: 511 GB, SQL Data F: 510 GB, SQL Log G: 510 GB, TempDB G: 63.6 GB.	
Servidor BDD Config	node	Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz Discos SO C: 80 GB, Backup E: 250 GB, SQL Data F: 250 GB, SQL Log G: 250 GB, TempDB G: 30 GB.	

Name	Type	Description	Properties
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.	
Trabajo de despliegue lappiz.com	technology-process		
Trabajo de despliegue: yaml	technology-process		
Trabajo de integración lappiz.com	technology-process		
Trabajo de integración: yaml	technology-process		

Documento de Relación de Tecnologías y Licenciamiento

Migracion.5. Licenciamiento

PGN. Migración Sistemas Misionales.
Fase 2.

Requisitos de licenciamiento de los
Módulos Central Sistema Único de
Información, SIU de PGN

versión 0.1.1

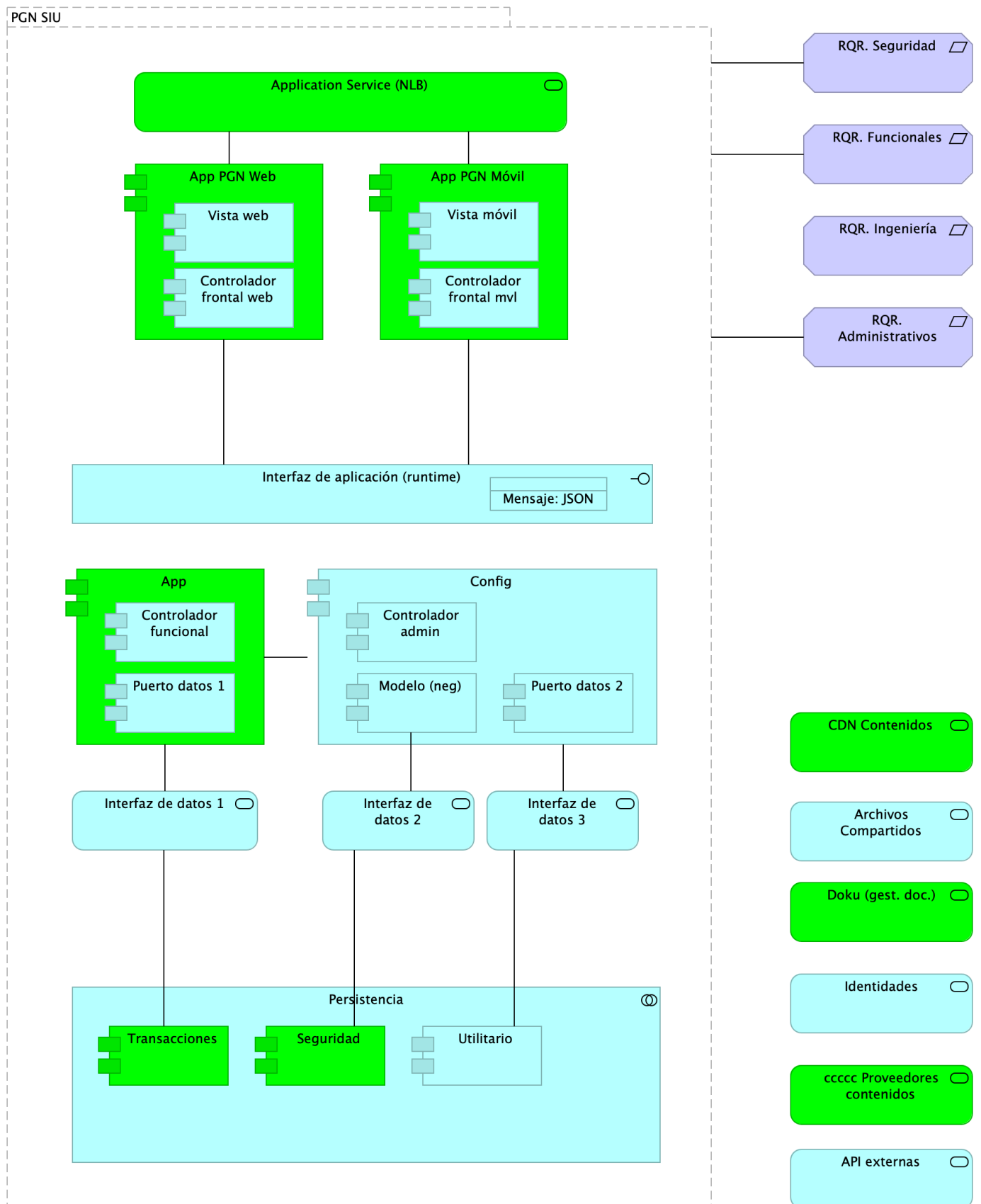


Imagen 12: Diagram: Migracion.5. Licenciamiento

Listado de los requisitos de licenciamiento a razón de los elementos usados por los módulos centrales del SIU Migrado, 2023.

Los elementos resaltados de la vista actual requieren modelos de licenciamiento variado, bien sea por usuario, núcleo, despliegue (instalación), o renta por consumo.

Catálogo de Elementos

Name	Type	Description	Properties
Persistencia	application-collaboration		
App	application-component		plataforma: node Js brecha: 100
App PGN Móvil	application-component	<p>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.</p> <p>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.</p> <p>La informacion contenida en las bases de datos debe tener los mecanismos de cifrado que en otros apartados se han mencionado.</p> <p>La legislación que hay que tener como referencia, ley 1581 de 2012. Decreto 1377 de 2013</p> <p>La metodología empleada tendrá las siguientes fases:</p> <ul style="list-style-type: none">• FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como: o Recopilación de dominios/IPs/puertos/servicios o Recopilación de metadatos o Uso de Google Dorks.• ANÁLISIS DE VULNERABILIDADES: Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.• EXPLOTACIÓN: • Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo: o Inyección de código o Inclusión de ficheros locales o remotos o Evasión de autenticación o Carencia de controles de autorización o Ejecución de comandos en el lado del servidor o Ataques tipo Cross Site Request Forgery o Control de errores o Gestión de sesiones o Fugas de información o Secuestros de sesión o Comprobación de las condiciones para realizar una denegación de servicio.• POST EXPLOTACIÓN: En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adiciones con el objetivo de comprobar la criticidad de esta. No URL IP 1. https://runtimetest.lappiz.io/#/auth/login/ PGN_Lappiz 135.181.185.207	plantilla: element-md-bold brecha: 100

Name	Type	Description	Properties
App PGN Web	application-component	<p>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 Ethical Hacking.</p> <p>Los resultados permitirán identificar los requisitos de seguridad que los sistemas de informacion o servicios web deberán cumplir.</p> <p>La metodologia empleada tendrá las siguientes fases:</p> <ul style="list-style-type: none"> • FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como: o Recopilación de dominios/IPs/puertos/servicios o Recopilación de metadatos o Uso de Google Dorks. • ANÁLISIS DE VULNERABILIDADES: Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades. • EXPLOTACIÓN: • Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo: o Inyección de código o Inclusión de ficheros locales o remotos o Evasión de autenticación o Carencia de controles de autorización o Ejecución de comandos en el lado del servidor o Ataques tipo Cross Site Request Forgery o Control de errores o Gestión de sesiones o Fugas de información o Secuestros de sesión o Comprobación de las condiciones para realizar una denegación de servicio. • POST EXPLOTACIÓN: En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adiciones con el objetivo de comprobar la criticidad de esta. No URL IP 1. https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz 135.181.185.207 El Login deberá evidenciar el control de errores, al momento de realizar la validación deberá mensaje de error para el caso que se autentique con credenciales erradas. 	<p>plataforma: angular 11 brecha: 100</p>
Config	application-component		plataforma: cs
Controlador admin	application-component		plataforma: cs
Controlador frontal mvl	application-component		plataforma: js
Controlador frontal web	application-component	<p>- Verificados los SSL, se recomienda adquirir SSL seguros, con entidades certificadoras.</p> <p>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.</p>	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

Name	Type	Description	Properties
Vista web	application-component	- Verificados los SSL, se recomienda adquirir SSL seguros, con entidades certificadoras. Si se desea continuar con SSL de Let's Encrypt, se recomienda automatizar el proceso de actualización dado que al dejar estos en modo actualización manual es probable el olvido de esta actualización (Estos certificados se deben actualizar trimestralmente y no cuentan con las características de seguridad necesarias. 4. SERVICIOS IDENTIFICADOS: Servidor web: Microsoft-IIS/10.0 Marco de Programación: ASP.NET Huellas digitales identificadas: Huella digital SHA-256 "FC:79:06:7E:F5:24:20:50:F1:C0:74:F7:85:56:B9:05:B7:33:A3:2D:44:A0:48" Huella digital SHA1 "8C:48:BD:E2:F5:18:18:C3:85:96:68:44:2E:28:A0:68:08:2F:0A:BE"	plataforma: html
Interfaz de aplicación (runtime)	application-interface	Servidor web: Microsoft-IIS/10.0 Marco de Programación: ASP.NET Huellas digitales identificadas: Huella digital SHA-256 "FC:79:06:7E:F5:24:20:50:F1:C0:74:F7:85:56:B9:05:B7:33:A3:2D:44:A0:48" Huella digital SHA1 "8C:48:BD:E2:F5:18:18:C3:85:96:68:44:2E:28:A0:68:08:2F:0A:BE"	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 conflicto entre ellos.	
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.	

Generated on: Thu Oct 19 2023 09:19:30 GMT-0500 (COT)

Arquitectura de Información (Datos)

- [Diagrama Modelo de Datos Conceptual](#)
 - [Migracion.2a.a1.Datos Lógico](#)
- [Diagrama Modelo de Datos Físico \(diagramas entidad-relación\)](#)
 - [Migracion.2a.a3. Datos Modelo Físico](#)
- [Diagrama Modelo de Datos Lógico](#)
 - [Migracion.2c. Datos Hominis](#)
 - [Migracion.2c3. Datos Control Interno](#)
 - [Migracion.2c2. Datos SIRI](#)
 - [Migracion.2c1. Datos SIM](#)
- [Documento Diccionarios de Datos](#)

- [Mapa de Información \(flujos de información\)](#)
 - [Migracion.2. datos](#)
- [Modelo Ontológico](#)

Diagrama Modelo de Datos Conceptual

Migracion.2a.a1.Datos Lógico

PGN. Migración Sistemas Misionales.
Fase 2.

Organización de las entidades
lógicas de datos de negocio.
Módulos Central Sistema Único de
Información.

versión 0.1

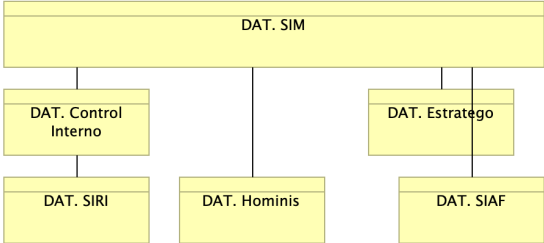


Imagen 13: Diagram: Migracion.2a.a1.Datos Lógico

Organización de los grupos de datos (dominios) del SUI Migrado, 2023.

Catálogo de Elementos

Name	Type	Description	Properties
DAT. Control Interno	business-object		
DAT. Estratégico	business-object	Entidades de datos de negocio de capital humano de la PGN. Sistema de información Homini.	
DAT. Hominis	business-object	Entidades de datos de negocio de capital humano de la PGN. Sistema de información Homini.	
DAT. SIAF	business-object	Entidades de datos de negocio de capital humano de la PGN. Sistema de información Homini.	
DAT. SIM	business-object		
DAT. SIRI	business-object		

Diagrama Modelo de Datos Físico (diagramas entidad-relación)

Migracion.2a.a3. Datos Modelo Físico

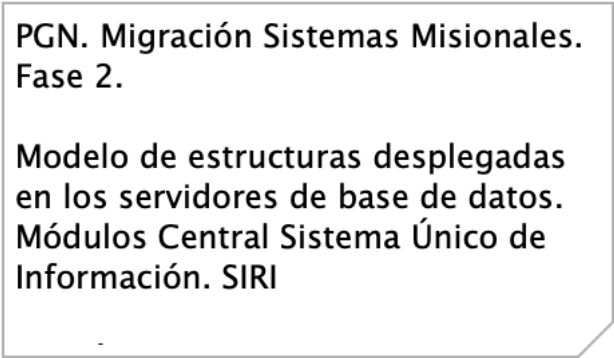


Imagen 14: Diagram: Migracion.2a.a3. Datos Modelo Físico

En contrucción.

Catálogo de Elementos

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

Diagrama Modelo de Datos Lógico

Migracion.2c. Datos Hominis

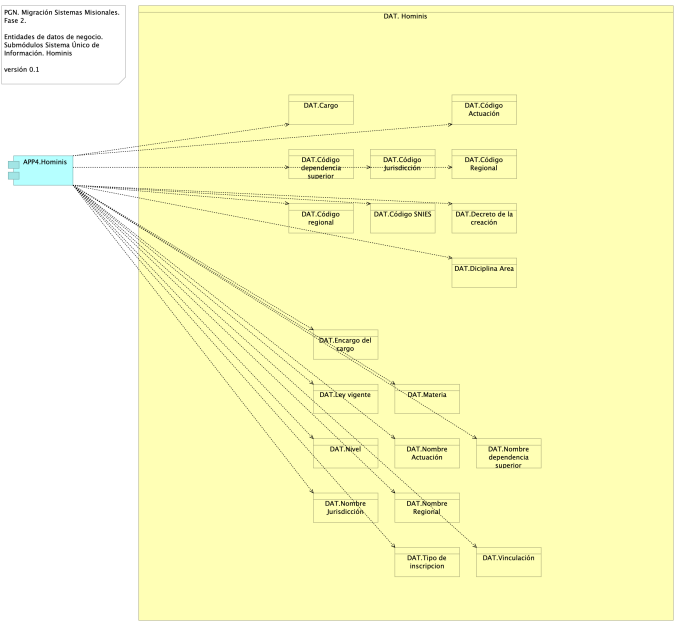


Imagen 15: Diagram: Migracion.2c. Datos Hominis

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

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

Catálogo de Elementos

Name	Type	Description	Properties
APP4.Hominis	application-component	Módulo del SUI. Gestión de capital humano, funcionarios y cargos de representación y libre remoción de la PGN.	
DAT. Hominis	business-object	Entidades de datos de negocio de capital humano de la PGN. Sistema de información Homini.	
DAT.Cargo	business-object		
DAT.Código Actuación	business-object		
DAT.Código Jurisdicción	business-object		
DAT.Código Regional	business-object		
DAT.Código SNIES	business-object		
DAT.Código dependencia superior	business-object		
DAT.Código regional	business-object		
DAT.Decreto de la creación	business-object		
DAT.Diciplina Area	business-object		
DAT.Encargo del cargo	business-object		
DAT.Ley vigente	business-object		
DAT.Materia	business-object		
DAT.Nivel	business-object		
DAT.Nombre Actuación	business-object		
DAT.Nombre Jurisdicción	business-object		
DAT.Nombre Regional	business-object		
DAT.Nombre dependencia superior	business-object		
DAT.Tipo de inscripcion	business-object		
DAT.Vinculación	business-object		

Migracion.2c3. Datos Control Interno

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

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

versión 0.1

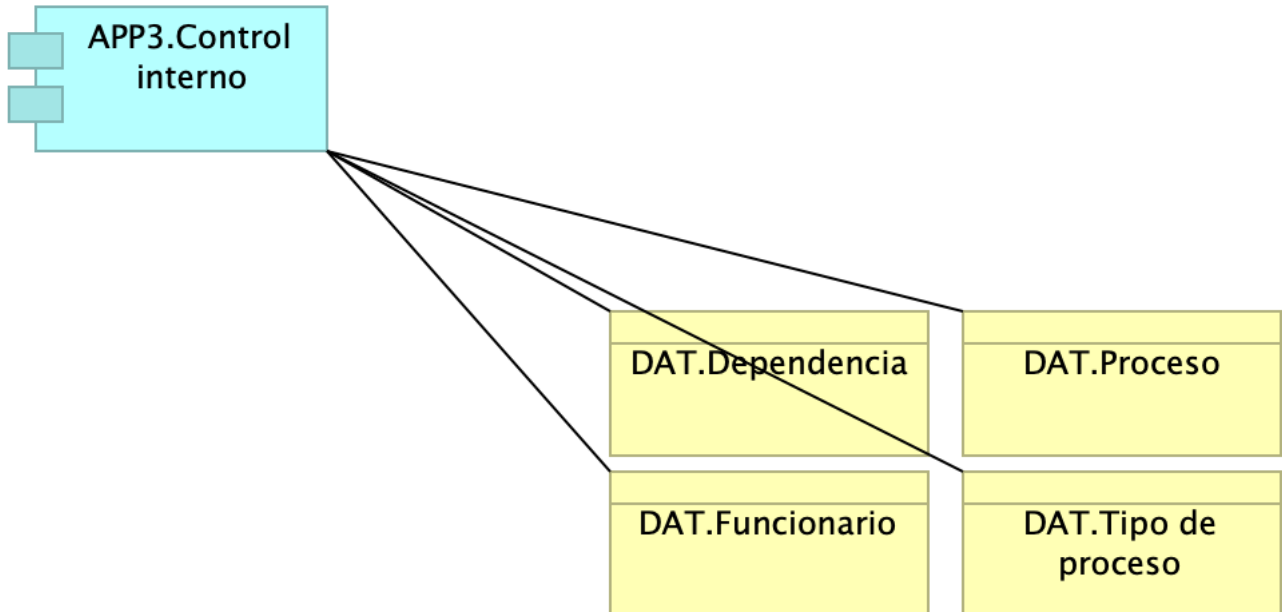


Imagen 16: Diagram: Migracion.2c3. Datos Control Interno

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

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

Catálogo de Elementos

Name	Type	Description	Properties
APP3.Control interno	application-component		
DAT.Dependencia	business-object		
DAT.Funcionario	business-object		
DAT.Proceso	business-object		
DAT.Tipo de proceso	business-object		

Migracion.2c2. Datos SIRI

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

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

versión 0.1

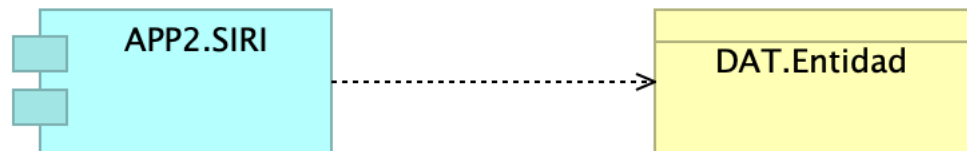


Imagen 17: Diagram: Migracion.2c2. Datos SIRI

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

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

Catálogo de Elementos

Name	Type	Description	Properties
APP2.SIRI	application-component		
DAT.Entidad	business-object		

Migracion.2c1. Datos SIM

PGN. Migración Sistemas Misionales.
Fase 2.

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

versión 0.1

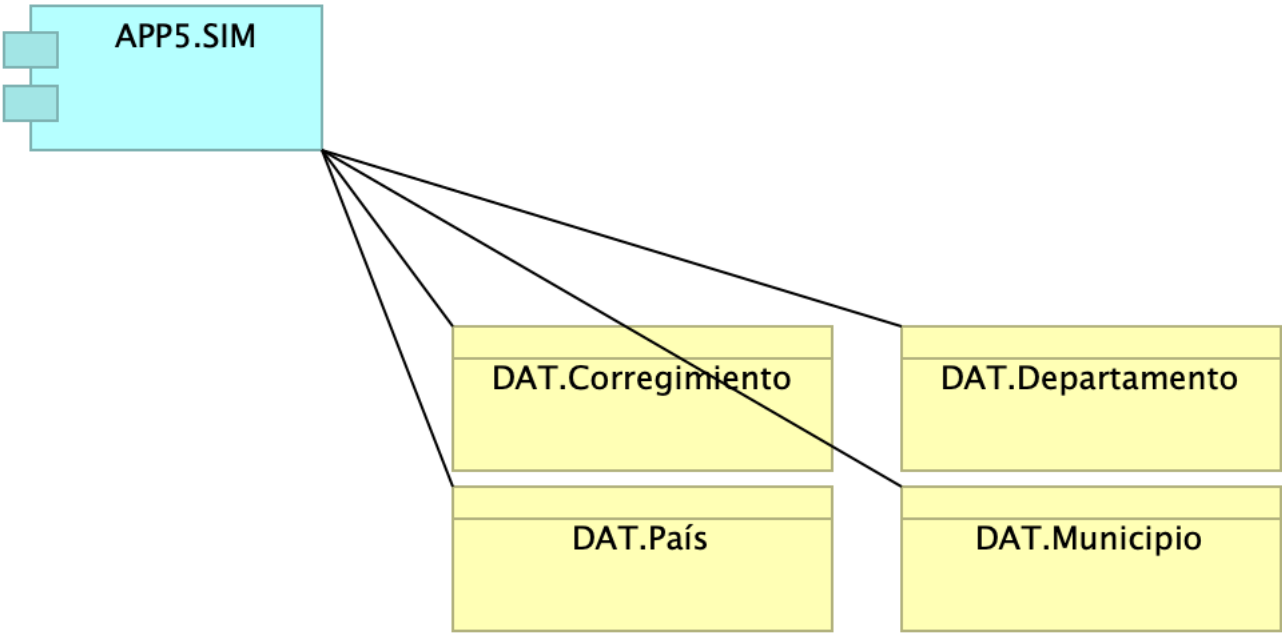


Imagen 18: Diagram: Migracion.2c1. Datos SIM

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

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

Catálogo de Elementos

Name	Type	Description	Properties
APP5.SIM	application-component		
DAT.Corregimiento	business-object		
DAT.Departamento	business-object		
DAT.Municipio	business-object		
DAT.País	business-object		

Documento Diccionarios de Datos

Mapa de Información (flujos de información)

Migracion.2. datos

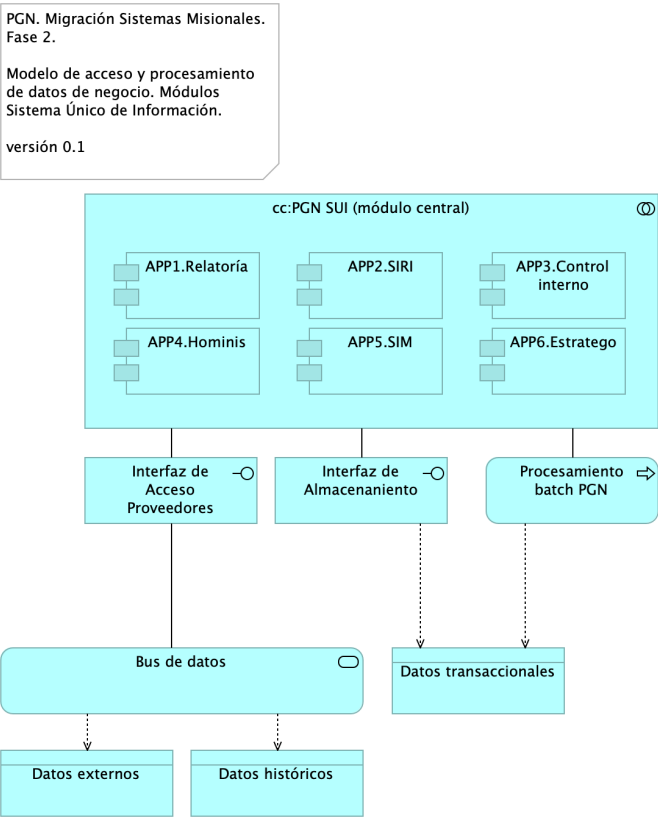


Imagen 19: Diagram: Migracion.2. datos

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

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

Consideramos tres tipos de 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 particular 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		
APP3.Control interno	application-component		
APP4.Hominis	application-component	Módulo del SUI. Gestión de capital humano, funcionarios y cargos de representación y libre remoción de la PGN.	
APP5.SIM	application-component		
APP6.Estratego	application-component		
Interfaz de Acceso Proveedores	application-interface	Interfaz de acceso a los tipos de datos externos al SUI.	
Interfaz de Almacenamiento	application-interface	Interfaz de acceso a los repositorio, base de datos relacionales y no jerárquicas. Tipos de datos transaccionales, internos, del SUI.	
Procesamiento batch PGN	application-process	Los procesos de lotes, que requieren volumenes de datos altos, deben hacer parte de la arquitectura de datos del SUI.	

Name	Type	Description	Properties
Bus de datos	application-service	El patrón de bus de datos tiene el rol de unir y referir a los datos externos al SUI de tal manera que hace transparente la localización y el formato de este tipo de datos.	
Datos externos	data-object		
Datos históricos	data-object		
Datos transaccionales	data-object		

Modelo Ontológico

Generated on: Thu Oct 19 2023 09:19:10 GMT-0500 (COT)

Arquitectura de Software: Infraestructura

- [Descripción de Infraestructura Migración SUI PGN](#)
 - [Lineabase.1a.SIU componentes. infraestructura](#)
 - [Lineabase.0.SIU aplicación. física](#)
 - [Seguridad.2. Lineabase.0.SIU Aplicación](#)

Descripción de Infraestructura Migración SUI PGN

Lineabase.1a.SIU componentes. infraestructura

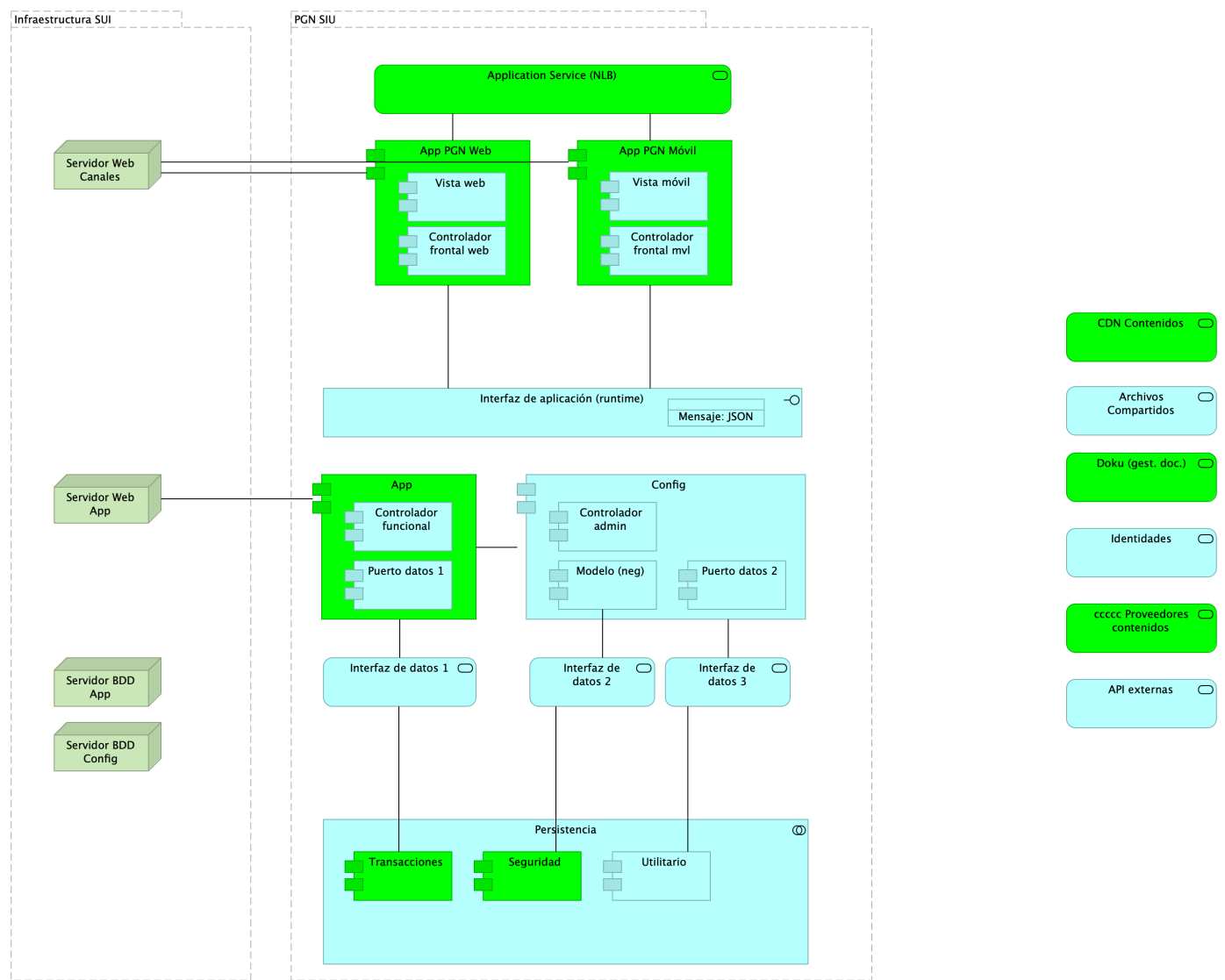


Imagen 20: Diagram: Lineabase.1a.SIU componentes. infraestructura

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

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

Catálogo de Elementos

Name	Type	Description	Properties
Persistencia	application-collaboration		
App	application-component		plataforma: node Js brecha: 100

Name	Type	Description	Properties
App PGN Móvil	application-component	<p>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.</p> <p>Protección de datos personales,</p> <p>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.</p> <p>La informacion contenida en las bases de datos debe tener los mecanismos de cifrado que en otros apartados se han mencionado.</p> <p>La legislación que hay que tener como referencia, ley 1581 de 2012. Decreto 1377 de 2013</p> <p>La metodologia empleada tendrá las siguientes fases:</p> <ul style="list-style-type: none">• FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como: o Recopilación de dominios/IPs/puertos/servicios o Recopilación de metadatos o Uso de Google Dorks.• ANÁLISIS DE VULNERABILIDADES: Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.• EXPLOTACIÓN: • Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo: o Inyección de código o Inclusión de ficheros locales o remotos o Evasión de autenticación o Carencia de controles de autorización o Ejecución de comandos en el lado del servidor o Ataques tipo Cross Site Request Forgery o Control de errores o Gestión de sesiones o Fugas de información o Secuestros de sesión o Comprobación de las condiciones para realizar una denegación de servicio.• POST EXPLOTACIÓN: En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adiciones con el objetivo de comprobar la criticidad de esta. <p>No URL IP 1. https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz 135.181.185.207</p>	<p><i>plantilla: element-md-bold</i> <i>brecha: 100</i></p>

Name	Type	Description	Properties
App PGN Web	application-component	<p>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 Ethical Hacking.</p> <p>Los resultados permitirán identificar los requisitos de seguridad que los sistemas de informacion o servicios web deberán cumplir.</p> <p>La metodologia empleada tendrá las siguientes fases:</p> <ul style="list-style-type: none"> • FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como: o Recopilación de dominios/IPs/puertos/servicios o Recopilación de metadatos o Uso de Google Dorks. • ANÁLISIS DE VULNERABILIDADES: Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades. • EXPLOTACIÓN: • Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo: o Inyección de código o Inclusión de ficheros locales o remotos o Evasión de autenticación o Carencia de controles de autorización o Ejecución de comandos en el lado del servidor o Ataques tipo Cross Site Request Forgery o Control de errores o Gestión de sesiones o Fugas de información o Secuestros de sesión o Comprobación de las condiciones para realizar una denegación de servicio. • POST EXPLOTACIÓN: En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adiciones con el objetivo de comprobar la criticidad de esta. No URL IP 1. https://runtime-test.lappiz.io/#/auth/login/ PGN_Lappiz 135.181.185.207 El Login deberá evidenciar el control de errores, al momento de realizar la validación deberá mensaje de error para el caso que se autentique con credenciales erradas. 	<p>plataforma: angular 11 brecha: 100</p>
Config	application-component		plataforma: cs
Controlador admin	application-component		plataforma: cs
Controlador frontal mvl	application-component		plataforma: js
Controlador frontal web	application-component	<p>- Verificados los SSL, se recomienda adquirir SSL seguros, con entidades certificadoras.</p> <p>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.</p>	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

Name	Type	Description	Properties
Vista web	application-component	<p>- Verificados los SSL, se recomienda adquirir SSL seguros, con entidades certificadoras.</p> <p>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.</p> <p>4. SERVICIOS IDENTIFICADOS:</p> <p>Servidor web: Microsoft-IIS/10.0</p> <p>Marco de Programación: ASP.NET</p> <p>Huellas digitales identificadas:</p> <p>Huella digital SHA-256</p> <p>"FC:79:06:7E:F5:24:20:50:F1:C0:74:F7:85:56:B9:05:B7:33:A3:2D:44:A0:48"</p> <p>Huella digital SHA1</p> <p>"8C:48:BD:E2:F5:18:18:C3:85:96:68:44:2E:28:A0:68:08:2F:0A:BE"</p>	plataforma: html
Interfaz de aplicación (runtime)	application-interface	<p>Servidor web: Microsoft-IIS/10.0</p> <p>Marco de Programación: ASP.NET</p> <p>Huellas digitales identificadas:</p> <p>Huella digital SHA-256</p> <p>"FC:79:06:7E:F5:24:20:50:F1:C0:74:F7:85:56:B9:05:B7:33:A3:2D:44:A0:48"</p> <p>Huella digital SHA1</p> <p>"8C:48:BD:E2:F5:18:18:C3:85:96:68:44:2E:28:A0:68:08:2F:0A:BE"</p>	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		
cccc Proveedores contenidos	application-service		brecha: 100
Mensaje: JSON	data-object		
Infraestructura SUI	grouping	<p>Soporte de infraestructura a los componentes del SUI Migración.</p> <p>Servidores y ambientes de cómputo para la ejecución del software base de los componentes misionales del SUI de PGN.</p>	
PGN SIU	grouping	<p>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.</p> <p>Los objetivos secundarios de esta arquitectura SUI de la migración son flexibilidad y extensibilidad. Dichos objetivos son independientes. Es decir, estos pueden ser maximizados sin conflicto entre ellos.</p>	
Servidor BDD App	node	<p>Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB.</p> <p>CPU 64 Bits, 4 Cores > 2 Ghz</p> <p>Discos SO C: 126 GB, Backup E: 511 GB, SQL Data F: 510 GB, SQL Log G: 510 GB, TempDB G: 63.6 GB.</p>	
Servidor BDD Config	node	<p>Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB.</p> <p>CPU 64 Bits, 4 Cores > 2 Ghz</p> <p>Discos SO C: 80 GB, Backup E: 250 GB, SQL Data F: 250 GB, SQL Log G: 250 GB, TempDB G: 30 GB.</p>	
Servidor Web App	node	<p>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.</p>	

Name	Type	Description	Properties
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.	

Lineabase.0.SIU aplicación. física

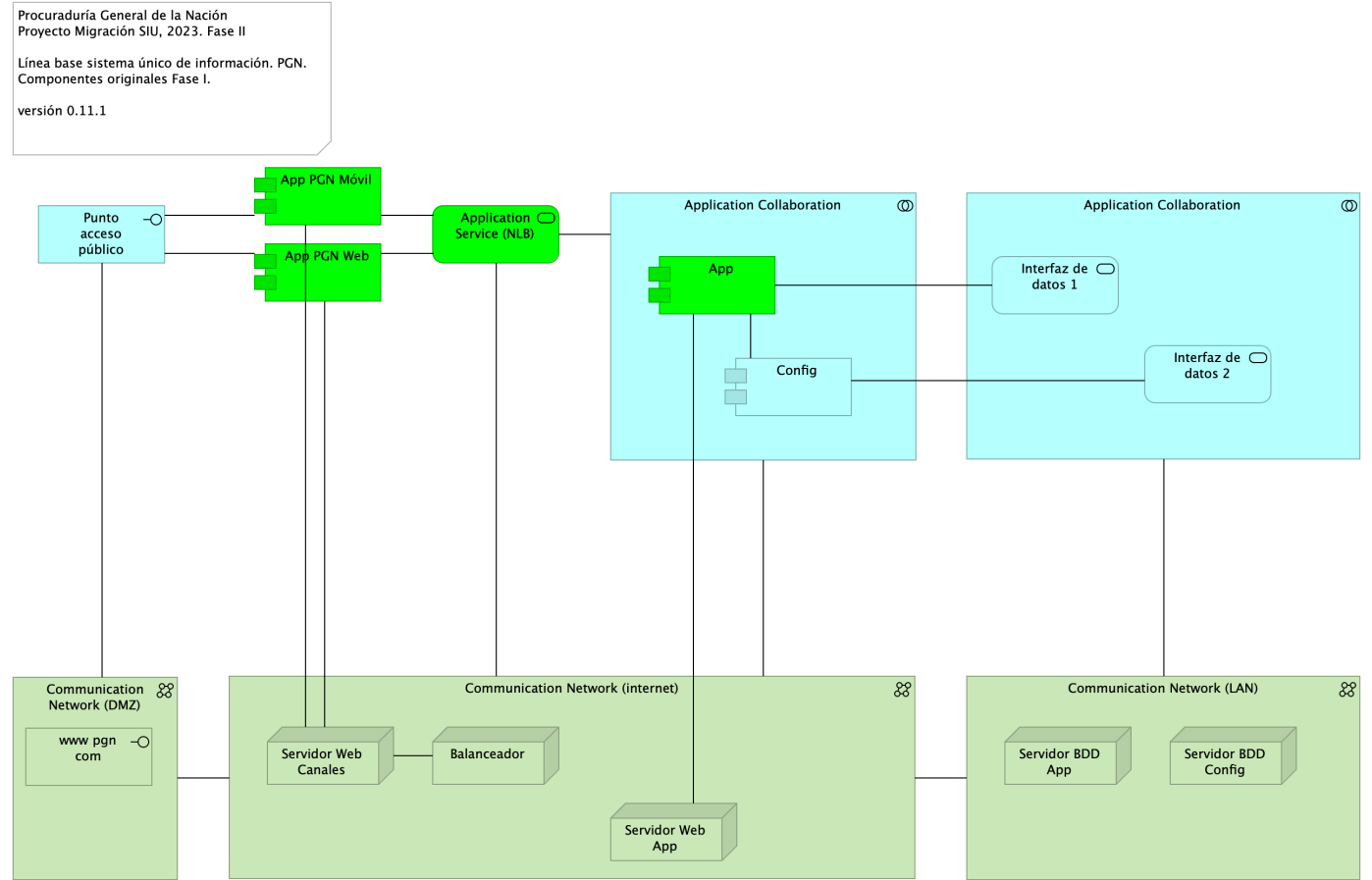


Imagen 21: Diagram: Lineabase.0.SIU aplicación. física

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

Representación Arquitectónica

Con una arquitectura orientada a servicios SUI recopila:

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

Catálogo de Elementos

Name	Type	Description	Properties
Application Collaboration	application-collaboration		
Application Collaboration	application-collaboration		
App	application-component		plataforma: node Js brecha: 100

Name	Type	Description	Properties
App PGN Móvil	application-component	<p>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.</p> <p>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.</p> <p>La informacion contenida en las bases de datos debe tener los mecanismos de cifrado que en otros apartados se han mencionado.</p> <p>La legislación que hay que tener como referencia, ley 1581 de 2012. Decreto 1377 de 2013</p> <p>La metodologia empleada tendrá las siguientes fases:</p> <ul style="list-style-type: none">• FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como: o Recopilación de dominios/IPs/puertos/servicios o Recopilación de metadatos o Uso de Google Dorks.• ANÁLISIS DE VULNERABILIDADES: Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.• EXPLOTACIÓN:<ul style="list-style-type: none">• Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo: o Inyección de código o Inclusión de ficheros locales o remotos o Evasión de autenticación o Carencia de controles de autorización o Ejecución de comandos en el lado del servidor o Ataques tipo Cross Site Request Forgery o Control de errores o Gestión de sesiones o Fugas de información o Secuestros de sesión o Comprobación de las condiciones para realizar una denegación de servicio.• POST EXPLOTACIÓN: En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adiciones con el objetivo de comprobar la criticidad de esta. <p>No URL IP 1. https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz 135.181.185.207</p>	<p><i>plantilla: element-md-bold</i> <i>brecha: 100</i></p>

Name	Type	Description	Properties
App PGN Web	application-component	<p>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 Ethical Hacking.</p> <p>Los resultados permitirán identificar los requisitos de seguridad que los sistemas de informacion o servicios web deberán cumplir.</p> <p>La metodologia empleada tendrá las siguientes fases:</p> <ul style="list-style-type: none"> • FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como: o Recopilación de dominios/IPs/puertos/servicios o Recopilación de metadatos o Uso de Google Dorks. • ANÁLISIS DE VULNERABILIDADES: Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades. • EXPLOTACIÓN: • Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo: o Inyección de código o Inclusión de ficheros locales o remotos o Evasión de autenticación o Carencia de controles de autorización o Ejecución de comandos en el lado del servidor o Ataques tipo Cross Site Request Forgery o Control de errores o Gestión de sesiones o Fugas de información o Secuestros de sesión o Comprobación de las condiciones para realizar una denegación de servicio. • POST EXPLOTACIÓN: En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adiciones con el objetivo de comprobar la criticidad de esta. No URL IP 1. https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz 135.181.185.207 El Login deberá evidenciar el control de errores, al momento de realizar la validación deberá mensaje de error para el caso que se autentique con credenciales erradas. 	<p>plataforma: angular 11 brecha: 100</p>
Config	application-component		plataforma: cs
Punto acceso público	application-interface	URL tipo C HTTP	
Application Service (NLB)	application-service		plataforma: angular 11 brecha: 100
Interfaz de datos 1	application-service		
Interfaz de datos 2	application-service		
Communication Network (DMZ)	communication-network		
Communication Network (LAN)	communication-network		
Communication Network (internet)	communication-network		
Balanceador	node		
Servidor BDD App	node	Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz Discos SO C: 126 GB, Backup E: 511 GB, SQL Data F: 510 GB, SQL Log G: 510 GB, TempDB G: 63.6 GB.	
Servidor BDD Config	node	Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz Discos SO C: 80 GB, Backup E: 250 GB, SQL Data F: 250 GB, SQL Log G: 250 GB, TempDB G: 30 GB.	

Name	Type	Description	Properties
Servidor Web App	node	Windows Server 2019 Standard o Datacenter x64. Nombre físico. IP LAN. IP Pública. Windows Server 2019 Standard or Datacenter x64. RAM 8 GB. CPU 64 Bits. 4 Cores de 2 Ghz. Discos SO C: 126 GB. SO D: 16 GB.	
Servidor Web Canales	node	Windows Server 2019 Standard o Datacenter x64. Nombre físico. IP LAN. IP Pública. Windows Server 2019 Standard or Datacenter x64. RAM 8 GB. CPU 64 Bits. 4 Cores de 2 Ghz. Discos SO C: 126 GB. SO D: 16 GB.	
www.pgn.com	technology-interface		

Seguridad.2. Lineabase.0.SIU Aplicación

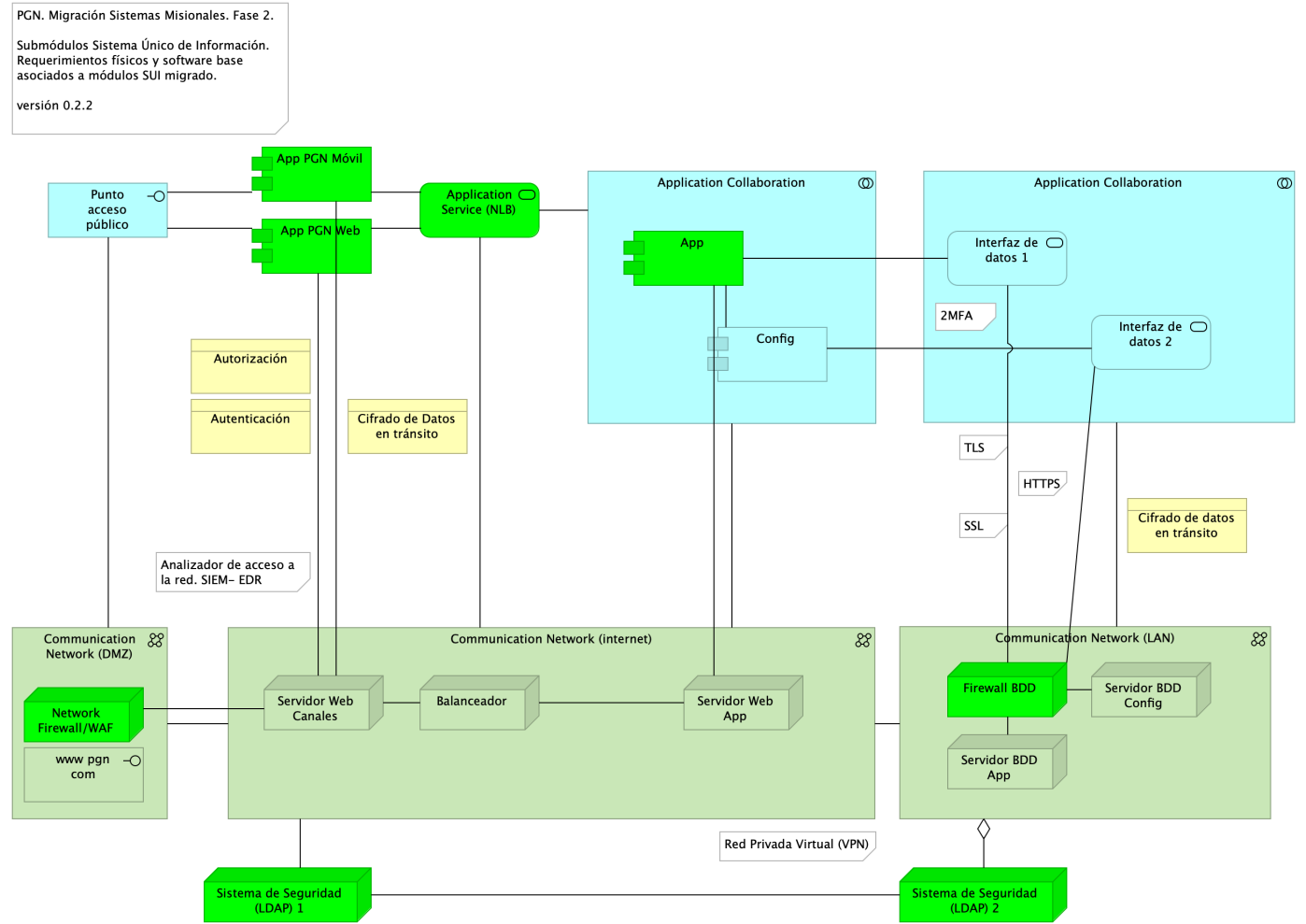


Imagen 22: Diagram: Seguridad.2. Lineabase.0.SIU Aplicación

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

Name	Type	Description	Properties
App PGN Móvil	application-component	<p>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.</p> <p>Protección de datos personales,</p> <p>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.</p> <p>La informacion contenida en las bases de datos debe tener los mecanismos de cifrado que en otros apartados se han mencionado.</p> <p>La legislación que hay que tener como referencia, ley 1581 de 2012. Decreto 1377 de 2013</p> <p>La metodologia empleada tendrá las siguientes fases:</p> <ul style="list-style-type: none">• FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como: o Recopilación de dominios/IPs/puertos/servicios o Recopilación de metadatos o Uso de Google Dorks.• ANÁLISIS DE VULNERABILIDADES: Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.• EXPLOTACIÓN:<ul style="list-style-type: none">• Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo: o Inyección de código o Inclusión de ficheros locales o remotos o Evasión de autenticación o Carencia de controles de autorización o Ejecución de comandos en el lado del servidor o Ataques tipo Cross Site Request Forgery o Control de errores o Gestión de sesiones o Fugas de información o Secuestros de sesión o Comprobación de las condiciones para realizar una denegación de servicio.• POST EXPLOTACIÓN: En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adiciones con el objetivo de comprobar la criticidad de esta. <p>No URL IP 1. https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz 135.181.185.207</p>	<p><i>plantilla: element-md-bold</i> <i>brecha: 100</i></p>

Name	Type	Description	Properties
App PGN Web	application-component	<p>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 Ethical Hacking.</p> <p>Los resultados permitirán identificar los requisitos de seguridad que los sistemas de informacion o servicios web deberán cumplir.</p> <p>La metodologia empleada tendrá las siguientes fases:</p> <ul style="list-style-type: none"> • FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como: o Recopilación de dominios/IPs/puertos/servicios o Recopilación de metadatos o Uso de Google Dorks. • ANÁLISIS DE VULNERABILIDADES: Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades. • EXPLOTACIÓN: • Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo: o Inyección de código o Inclusión de ficheros locales o remotos o Evasión de autenticación o Carencia de controles de autorización o Ejecución de comandos en el lado del servidor o Ataques tipo Cross Site Request Forgery o Control de errores o Gestión de sesiones o Fugas de información o Secuestros de sesión o Comprobación de las condiciones para realizar una denegación de servicio. • POST EXPLOTACIÓN: En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adiciones con el objetivo de comprobar la criticidad de esta. No URL IP 1. https://runtime-test.lappiz.io/#/auth/login/PGN_Lappiz135.181.185.207 El Login deberá evidenciar el control de errores, al momento de realizar la validación deberá mensaje de error para el caso que se autentique con credenciales erradas. 	<p>plataforma: angular 11 brecha: 100</p>
Config	application-component		plataforma: cs
Punto acceso público	application-interface	URL tipo C HTTP	
Application Service (NLB)	application-service		plataforma: angular 11 brecha: 100
Interfaz de datos 1	application-service		
Interfaz de datos 2	application-service		

Name	Type	Description	Properties
Autenticación	business-object	<p>Con el objetivo de incrementar el nivel de seguridad, para el proceso de autenticación se tendrán en cuenta las siguientes consideraciones:</p> <p>Validación del proceso de gestión de usuarios: La fortaleza de la autenticación dependerá del proceso de gestión de usuarios implementado por parte de la entidad. Se debe tener en cuenta los lineamientos definidos en la política Específica de Control de Acceso.</p> <p>Autenticación con integración de Windows: La autenticación permitirá que los usuarios asignados al dominio, una vez que se ingresen las credenciales, y realizada la validación, se autorizará el acceso a los servicios y/o soluciones a partir de la integración del directorio activo con la integración del LDAP – (Lightweight Directory Access Protocol).</p> <p>Los tipos de autenticación realizadas a partir de las identidades administradas de los recursos de Azure, entidades de Servicio y Certificados, podrán ser integrado con los dominios del directorio activo (DA) local. Por lo que respecta a la autenticación, será generado con la asignación de usuarios y credenciales definidas alineadas con la política Específica de Control de Acceso., a partir de la integración será validado el ingreso a las diferentes soluciones y/o sistemas de información de la PGN.</p> <p>Manejo y uso de contraseñas: Los servidores públicos deberán tener en cuenta los lineamientos definidos para la creación y gestión de contraseñas del Sistema de Gestión de Seguridad de la Información SGSI de la Procuraduría General de la Nación.</p> <p>Utilización de canales cifrados: El proceso de autenticación tendrá mecanismos de transmisión seguro. El uso del TLS (Transport Layer Security), será necesario para el acceso a la página de autenticación que ayude a garantizar la autenticidad de la aplicación a los funcionarios, como en la transmisión de las credenciales.</p> <p>Bloqueo de cuentas: Aquellas cuentas sobre las que se han realizados múltiples intentos de conexiones fallidas, cinco (5) intentos erróneos, se tendrá implementado un bloqueo temporal o permanente como mecanismo de seguridad para evitar amenazas de ataques.</p>	
Autorización	business-object	<p>Metodología</p> <p>Los mecanismos de autorización para el acceso a los sistemas de información de la procuraduría general de la nación describen la forma de cómo se restringe el acceso a los diferentes módulos (Misionales (SIM), Registros de Inhabilidades (SIRI), Nómina, Control Interno y relatoría, entre otros.), y que se considera un mecanismo de protección, que ayuda a reaccionar ante cualquier operación no autorizada. El control de acceso basado en roles (RBAC), enfoca la idea de que a los funcionarios se les otorgue los permisos de acceso a los recursos, basados en los roles y/o perfiles que este posee. Este control posee dos características fundamentales: i) los accesos son controlados por medio de los roles y/o perfiles asignados, quiere decir, a los servidores públicos, contratistas, terceros y otros colaboradores autorizados para interactuar con los sistemas de información se le asignan los roles y el encargado/responsable definirá los permisos, que a su vez están relacionados con los roles, ii) Los roles pueden ser definidos a nivel jerárquico, es decir que un rol podrá ser miembro de otro rol.</p> <p>Un proceso de autorización basado en roles, identifica tres factores importantes, i) Todos los servidores públicos, contratistas, terceros y otros Colaboradores, deben tener un rol asignado, si no es asignado no podrá realizar ninguna acción relacionada con el acceso, ii) un usuario podrá hacer uso de</p>	

Name	Type	Description	Properties
		<p>los permisos asociados a los roles asignados, el cual deberá realizar el inicio de sesión el usuario asignado del Directorio activo (DA), iii) los servidores públicos, contratistas, terceros y otros, solo podrán realizar acciones para las cuales han sido autorizados por medio de la activación de sus roles y/o perfiles.</p> <p>EL control definido para los accesos basados en roles RBAC, permitirá que solo las personas autorizadas de la PGN podrán acceder a ciertos recursos (programas, equipos, aplicaciones, bases de datos, etc.) definido por sus funciones laborales, lo que permitirá controlar los accesos desde diferentes escenarios: Sistemas de información, redes y aplicaciones.</p> <p>Gestión de identidades y Control de acceso:</p> <p>Gestor de identidades: En esta gestión se planifica el ciclo de vida de las identidades de usuario y se realizan los procesos de sincronización, de acuerdo a los suministros de accesos establecidos por la entidad, los cuales son integrados con el servidor que gestiona la identidad y control de acceso.</p> <p>Gestor de roles: La asignación de roles es sincronizada con la identidad de usuario en el servidor de dominio. Para esta gestión se crean las reglas y condiciones que determinan si un usuario puede o no pertenecer a un rol definido por la entidad.</p> <p>Para el gobierno y gestión de identidades y de acceso, se identificó como primera medida la implementación de la siguiente metodología.</p> <p>REGLAS PARA LA CREACIÓN DE USUARIOS.</p> <p>Identificación de Mecanismos:</p> <p>En este ítem se deben identificar las herramientas con las que cuenta la entidad, las cuales deberán ser registradas en el documento denominado: "Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_1 (Mecanismos)".</p> <p>Identificación de Roles y Privilegios</p> <p>Este ítem proporciona al sistema la definición de las políticas organizacionales en cuanto a la definición de los privilegios y roles de los diferentes actores en cada uno de los aplicativos con los que estos interactúan dentro de sus funciones, registradas en el documento denominado: "Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_2 (Roles)".</p> <p>Aprovisionamiento de cuentas</p> <p>Este ítem establece el proceso adecuado para el aprovisionamiento y desaprovisionamiento de cuentas de usuarios en las diferentes aplicaciones, permitiendo toda la gestión de ellas por medio de un sistema de directorio único y centralizado, Este aprovisionamiento se encuentra registrado en el documento denominado: "Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_4 y Hoja_5 (Permisos)".</p> <p>Establecimiento de mecanismos de control de acceso:</p> <p>Este ítem controla que usuarios tienen permitido el acceso a los diferentes aplicativos o herramientas dentro de la organización permitiendo segregar las funciones dependiendo del rol del usuario en cada sistema, Este establecimiento se encuentra registrado en el documento denominado: "Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_3 (Acceso)".</p> <p>Definición de Privilegios y accesos.</p> <p>Los accesos y privilegios serán identificados en la matriz, encargado identificar cada uno de los roles y perfiles que se tendrá cada usuario hacia los sistemas de información cumpliendo con el principio del menor privilegio, teniendo en cuenta que los usuarios deberán tener exclusivamente los permisos y privilegios que necesita para el desarrollo de sus actividades. La matriz identificará i) los roles que se deben crear para cada sistema de información, ii) los privilegios que requiere cada rol del sistema y iii) los</p>	

Name	Type	Description	Properties
		<p>niveles de accesos requeridos, (Consultar, Modificar, Eliminar) (CRUD) y iv) Tipos de usuarios, roles que pueden ser asignados al perfil, entre otros.</p> <p>Configuración de permisos</p> <p>La configuración con de los perfiles con sus accesos y privilegios en los sistemas de información se debe realizar empleando las herramientas propias de la procuraduría general de la nacional PGN, y serán asignados los permisos según la matriz de roles y permisos.</p> <p>Identificación de Mecanismos:</p> <p>En este ítem se deben identificar las herramientas con las que cuenta la entidad, las cuales deberán ser registradas en el documento denominado:</p> <p>“Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_1 (Mecanismos)”.</p> <p>Identificación de Roles y Privilegios</p> <p>Este ítem proporciona al sistema la definición de las políticas organizacionales en cuanto a la definición de los privilegios y roles de los diferentes actores en cada uno de los aplicativos con los que estos interactúan dentro de sus funciones, registradas en el documento denominado:</p> <p>“Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_2 (Roles)”.</p> <p>Aprovisionamiento de cuentas</p> <p>Este ítem establece el proceso adecuado para el aprovisionamiento y des aprovisionamiento de cuentas de usuarios en las diferentes aplicaciones, permitiendo toda la gestión de ellas por medio de un sistema de directorio único y centralizado, Este aprovisionamiento se encuentra registrado en el documento denominado:</p> <p>“Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_4 y Hoja_5 (Permisos)”.</p> <p>Establecimiento de mecanismos de control de acceso:</p> <p>Este ítem controla que usuarios tienen permitido el acceso a los diferentes aplicativos o herramientas dentro de la organización permitiendo segregar las funciones dependiendo del rol del usuario en cada sistema, Este establecimiento se encuentra registrado en el documento denominado: “Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_3 (Acceso)”.</p> <p>Definición de Privilegios y accesos.</p> <p>Los accesos y privilegios serán identificados en la matriz, encargado identificar cada uno de los roles y perfiles que se tendrá cada usuario hacia los sistemas de información cumpliendo con el principio del menor privilegio, teniendo en cuenta que los usuarios deberán tener exclusivamente los permisos y privilegios que necesita para el desarrollo de sus actividades. La matriz identificará i) los roles que se deben crear para cada sistema de información, ii) los privilegios que requiere cada rol del sistema y iii) los niveles de accesos requeridos, (Consultar, Modificar, Eliminar) (CRUD) y iv) Tipos de usuarios, roles que pueden ser asignados al perfil, entre otros.</p> <p>Configuración de permisos</p> <p>La configuración con de los perfiles con sus accesos y privilegios en los sistemas de información se debe realizar empleando las herramientas propias de la procuraduría general de la nacional PGN, y serán asignados los permisos según la matriz de roles y permisos.</p>	

Name	Type	Description	Properties
Cifrado de Datos en tránsito	business-object	<p>Proteger la información propia de la PGN utilizando mecanismos de cifrado que permita garantizar los pilares de Seguridad de la Información Confidencialidad e integridad, asimismo reducir los riesgos de la información mediante la ayuda de Técnicas Criptograficas.</p> <p>Como mecanismos se propone implementar estos mecanismos de cifrado, como el protocolo TLS (Transport Layer Security) que permite a dos partes identificarse y autenticarse entre sí y comunicarse con confidencialidad e integridad de datos a partir de la conexión del usuario y un servidor WEB.</p> <p>Se propone integrar certificados SSL, que permite cifrar la información confidencial a fin de que solo los autorizados puedan tener acceso a ella, y así evitar manipulación de información confidencial.</p> <p>La Seguridad que brinda SSL, da garantía para acceder a los aplicativos de PNG.</p> <p>Como implementar certificados SSL?</p> <p>Podrán ser adquiridos a través del proveedor de dominios.</p> <p>TLS el protocolo que surge para reforzar la seguridad de los certificados SSL, que funciona como mecanismo de encriptación para que sea realmente transparente el envío de la información, proporcionando una autenticación sólida, restringiendo la manipulación, interceptación y alteración de mensajes.</p> <p>La última versión del TLS es la 1.3</p>	
Cifrado de datos en tránsito	business-object	<p>Proteger la información propia de la PGN utilizando mecanismos de cifrado que permita garantizar los pilares de Seguridad de la Información Confidencialidad e integridad, asimismo reducir los riesgos de la información mediante la ayuda de Técnicas Criptograficas. Como mecanismos se propone implementar estos mecanismos de cifrado, como el protocolo TLS (Transport Layer Security) que permite a dos partes identificarse y autenticarse entre sí y comunicarse con confidencialidad e integridad de datos a partir de la conexión del usuario y un servidor WEB.</p> <p>Se propone integrar certificados SSL, que permite cifrar la información confidencial a fin de que solo los autorizados puedan tener acceso a ella, y así evitar manipulación de información confidencial.</p> <p>La Seguridad que brinda SSL, da garantía para acceder a los aplicativos de PNG.</p> <p>Como implementar certificados SSL?</p> <p>Podrán ser adquiridos a través del proveedor de dominios.</p> <p>TLS el protocolo que surge para reforzar la seguridad de los certificados SSL, que funciona como mecanismo de encriptación para que sea realmente transparente el envío de la información, proporcionando una autenticación sólida, restringiendo la manipulación, interceptación y alteración de mensajes.</p> <p>La última versión del TLS es la 1.3</p>	
Communication Network (DMZ)	communication-network		
Communication Network (LAN)	communication-network		
Communication Network (Internet)	communication-network		
Balanceador	node		
Firewall BDD	node		<i>brecha:</i> 100
Network Firewall/WAF	node		<i>brecha:</i> 100
Servidor BDD App	node	<p>Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB.</p> <p>CPU 64 Bits, 4 Cores > 2 Ghz</p> <p>Discos SO C: 126 GB, Backup E: 511 GB, SQL Data F: 510 GB, SQL Log G: 510 GB, TempDB G: 63.6 GB.</p>	
Servidor BDD Config	node	<p>Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB.</p> <p>CPU 64 Bits, 4 Cores > 2 Ghz</p> <p>Discos SO C: 80 GB, Backup E: 250 GB, SQL Data F: 250 GB, SQL Log G: 250 GB, TempDB G: 30 GB.</p>	

Name	Type	Description	Properties
Servidor Web App	node	Windows Server 2019 Standard o Datacenter x64. Nombre físico. IP LAN. IP Pública. Windows Server 2019 Standard or Datacenter x64. RAM 8 GB. CPU 64 Bits. 4 Cores de 2 Ghz. Discos SO C: 126 GB. SO D: 16 GB.	
Servidor Web Canales	node	Windows Server 2019 Standard o Datacenter x64. Nombre físico. IP LAN. IP Pública. Windows Server 2019 Standard or Datacenter x64. RAM 8 GB. CPU 64 Bits. 4 Cores de 2 Ghz. Discos SO C: 126 GB. SO D: 16 GB.	
Sistema de Seguridad (LDAP) 1	node	Sistema de Seguridad (LDAP) 1. Control de acceso internet, La autenticación podrá estar integrada con el directorio activo, a partir de la generación de código para el ingreso con 2FA, que podrá generar un código la plataforma de correo corporativo, el cual solicitará el código de autenticación y una vez ingresado podrá redirigir al sitio.	brecha: 100
Sistema de Seguridad (LDAP) 2	node	Sistema de Seguridad (LDAP) 2. Control de acceso internet, La solución se podrá integrar con el directorio activo, a partir de la generación del 2FA, que podrá generar un código por desde la plataforma de office 365, el cual solicitará el código de autenticación y una vez ingresado podrá acceder al sitio.	brecha: 100
www.pgn.com	technology-interface		

Generated on: Thu Oct 19 2023 09:18:43 GMT-0500 (COT)

Requerimientos de Administración

- 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.
- 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.
- 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.
- Administrar los Permisos de acceso: Esta funcionalidad permite definir específicamente a que servicios de la solución puede ingresar un usuario (CRUD).
- 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.
- Las soluciones deben permitir la configuración de permisos de consulta con diferentes alcances para cada tipo de usuario.
- Desde la interfaz de usuario se debe poder crear, modificar o inactivar usuarios, perfiles o roles, permisos a las diferentes funcionalidades de la solución.
- Las soluciones deben permitir la definición de varios tipos de usuario.
- Las soluciones deben permitir la parametrización de los consecutivos que maneja la entidad para los diferentes documentos generados por las soluciones.
- Debe permitir parametrizar la vinculación del consecutivo a un documento en forma manual o automática.
- 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

- 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.
- 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.
- 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.
- 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.
- 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.
- La solución debe proveer una consulta que permita a un usuario con los privilegios asignados, consultar los registros de auditoría, aplicando criterios de filtro (usuario, máquina, rango de fechas y tipo de operación).

7. Las soluciones deben integrarse con LDAP – (Lightweight Directory Access Protocol) para los procesos de inicio de sesión y autenticación. La solución debe soportar la integración Nativa con Active Directory de Microsoft. Para usuarios externos el mecanismo de autorización, autenticación y acceso será controlado a través del modelo de seguridad de la solución (no habrá autenticación para usuarios externos).
8. Las soluciones deben cumplir con los lineamientos de seguridad relacionados a su utilización a través de redes públicas y privadas, garantizando la confidencialidad e integridad de la información y acceso a ella.
9. Debe evidenciar que, a través de pruebas de vulnerabilidad, garantiza la seguridad de la información. Estas pruebas deben suministrar evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad.
10. Debe incluir un mecanismo de cifrado de los datos que se transportan entre los diferentes componentes tecnológicos y los datos sensibles de la base de datos que representen un alto nivel de confidencialidad.
11. A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio).
12. Debe contemplar el cumplimiento de la normatividad vigente en cuanto a protección de datos personales y debe permitir el manejo de excepciones.
13. Para los casos que aplique se debe permitir el manejo de certificados y/o firmas digitales en los documentos que así se definan para efectos de aprobación y digitalización.
14. Debe contemplar las prácticas de desarrollo seguro de aplicaciones y/o implementación segura de productos, para su naturaleza Web based.
15. Debe funcionar sobre protocolo SSL (certificados internos de la entidad cuando los sistemas de información sean internas y certificados validos públicamente cuando los sistemas de información estén expuestas a internet).
16. Debe entregar un procedimiento para el respaldo de la información de acuerdo con las necesidades de la entidad.
17. Debe incluir uso de criptografía para transacciones y/o campos sensibles según lo indiquen las normas vigentes y las necesidades específicas del negocio de acuerdo como lo determine la entidad.
18. Debe contemplar un modelo de datos que garantice base de datos única para evitar que se pueda presentar duplicidad de información.
19. En la información confidencial solo puede ser consultada por los perfiles autorizados e igualmente restringir documentos de consulta según los privilegios o permisos asociados.
20. A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio).
21. Debe cerrar las transacciones luego de máximo 10 minutos de inactividad.
22. Debe incluir controles de bloqueo de cuenta después de un máximo de 5 intentos erróneos a fin de evitar ataques de fuerza bruta.
23. Debe evidenciar el resultado positivo frente a pruebas de ethical hacking, análisis de vulnerabilidades, carga, estrés y desempeño antes de la puesta en operación de acuerdo con los lineamientos de la entidad.
24. Debe cumplir con todos los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la “Guía de desarrollo OWASP” y “OWAS Cheat Sheet”.

Referencias

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

1. **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/>