


# Documento de Arquitectura Migración Funcional PGN SIU

*Los productos de esta etapa, Migración Funcional SIU, Contrato 078-2023, ([Web](#)) están basados en el resultado de la Fase 1 del proyecto PGN SIU del 2022, [Sharepoint Softgic@37e52a6](#) del September 11, 2023.*

**Versión** del producto 1.37e52a6 de 11 Sep 2023

## Autores

---

- **Harry Wong, ing.**
  -  Usuario [e\\_hwong](#)  
Arquitecto, Softgic

✉ — Enviar mensajes a Harry Wong, ing. <[harry.wong@softgic.co](mailto: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.

# Control de Cambios

---

Tema	078-2023 Fase 2, PGN Migración Funcional SIU
Palabras clave	SIU, Softgic, PGN, Análisis de brecha, GAP, Comparativa
Autor	
Fuente	
Versión	1.37e52a6 del 11 Sep 2023
Vínculos	<a href="#">N003a Vista Segmento PGN SIU</a>

# Documento de Arquitectura Migración SUI

---

- [Línea Base PGN SIU](#)
  - [Lineabase.0.SIU aplicación](#)
  - [Lineabase.1.SIU componente](#)
  - [Lineabase.1a.SIU componentes. infraestructura](#)
  - [Lineabase.2.Portal](#)
  - [Riesgos.1. Migración funcional](#)
- [Arquitectura Migración PGN SIU](#)
  - [Migracion.1a.SIU submodulos](#)
  - [Migracion.1c.SIU submódulos componentes](#)
  - [Migracion.1b.SIU submodulos colaboración](#)
- [Organización cambios arquitectura](#)
  - [Organización. 1n. Mapa producto](#)
  - [Organización. 1n.1. Mapa producto PGN. Relatoría](#)
- [Arquitectura de Seguridad, SUI Migración](#)
  - [Seguridad. 1. Requerimientos](#)
  - [Seguridad. Lineabase.2.Portal](#)

# Línea Base PGN SIU

## Lineabase.0.SIU aplicación

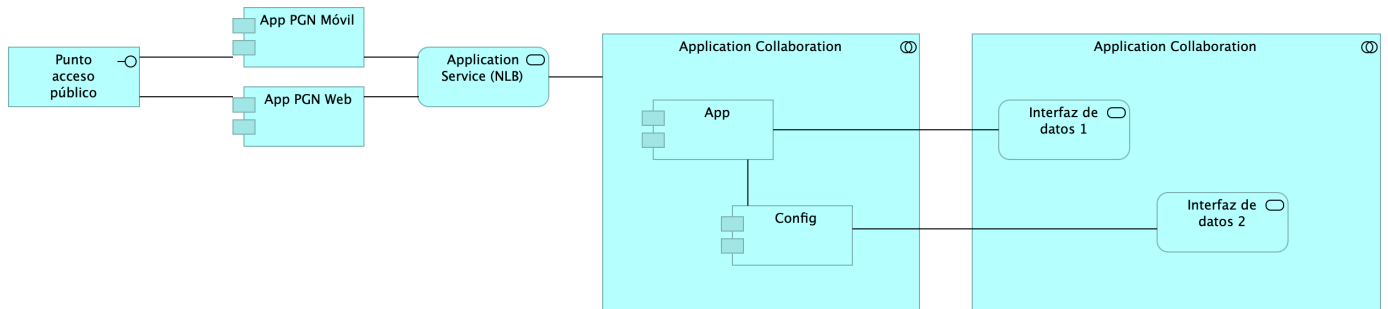


Imagen 1: Diagram: Lineabase.0.SIU aplicación

## Representación Arquitectónica

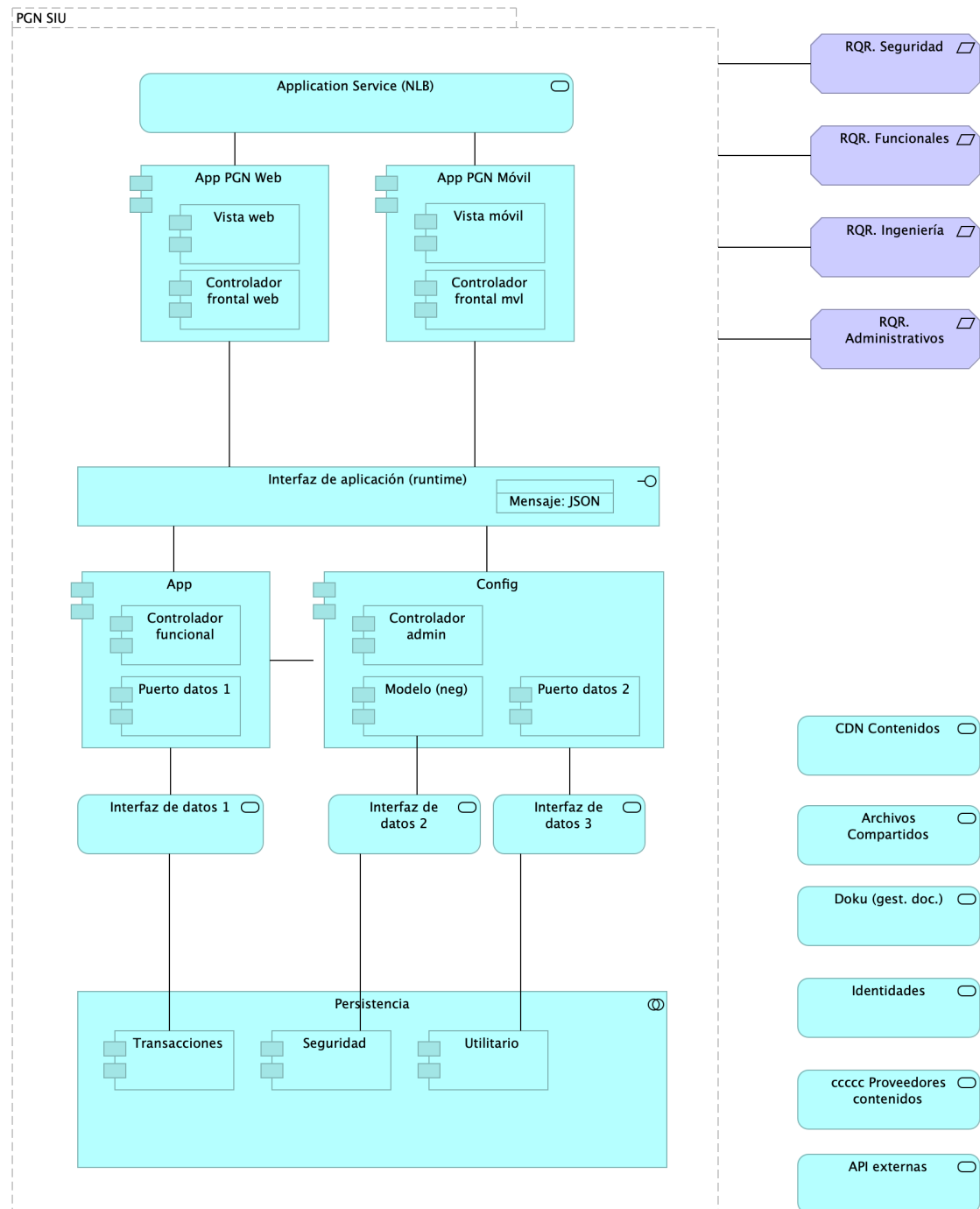
Con una arquitectura orientada a servicios SUI recopilamos:

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
App PGN Móvil	application-component		
App PGN Web	application-component		plataforma: angular 11
Config	application-component		plataforma: cs
Punto acceso público	application-interface	URL tipo C HTTP	
Application Service (NLB)	application-service		plataforma: angular 11
Interfaz de datos 1	application-service		
Interfaz de datos 2	application-service		

## Lineabase.1.SIU componente



**Imagen 2:** Diagram: Lineabase.1.SIU componente

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

Cuatro paquetes con tecnologías respectivas

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

Asuntos de la Migración:

- Estrategia CMS central
- Motor de búsqueda
- Estatego como BI

- Conciliación y Doku
- Gestión de sesiones / caducidad

## Catálogo de Elementos

Name	Type	Description	Properties
<b>Persistencia</b>	application-collaboration		
<b>App</b>	application-component		<i>plataforma:</i> node js
<b>App PGN Móvil</b>	application-component		
<b>App PGN Web</b>	application-component		<i>plataforma:</i> angular 11
<b>Config</b>	application-component		<i>plataforma:</i> cs
<b>Controlador admin</b>	application-component		<i>plataforma:</i> cs
<b>Controlador frontal mvl</b>	application-component		<i>plataforma:</i> js
<b>Controlador frontal web</b>	application-component		<i>plataforma:</i> js
<b>Controlador funcional</b>	application-component		<i>plataforma:</i> js
<b>Modelo (neg)</b>	application-component		<i>plataforma:</i> cs
<b>Puerto datos 1</b>	application-component		<i>plataforma:</i> js
<b>Puerto datos 2</b>	application-component		<i>plataforma:</i> cs
<b>Seguridad</b>	application-component		<i>plataforma:</i> sql
<b>Transacciones</b>	application-component		<i>plataforma:</i> sql
<b>Utilitario</b>	application-component		<i>plataforma:</i> no-sql
<b>Vista móvil</b>	application-component		<i>plataforma:</i> js
<b>Vista web</b>	application-component		<i>plataforma:</i> html
<b>Interfaz de aplicación (runtime)</b>	application-interface		<i>plataforma:</i> angular 11
<b>API externas</b>	application-service		
<b>Application Service (NLB)</b>	application-service		<i>plataforma:</i> angular 11
<b>Archivos Compartidos</b>	application-service		
<b>CDN Contenidos</b>	application-service		
<b>Doku (gest. doc.)</b>	application-service		
<b>Identidades</b>	application-service		
<b>Interfaz de datos 1</b>	application-service		
<b>Interfaz de datos 2</b>	application-service		
<b>Interfaz de datos 3</b>	application-service		
<b>cccc Proveedores contenidos</b>	application-service		
<b>Mensaje: JSON</b>	data-object		

Name	Type	Description	Properties
<b>PGN SIU</b>	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.	
<b>RQR. Administrativos</b>	requirement		
<b>RQR. Funcionales</b>	requirement		
<b>RQR. Ingeniería</b>	requirement		
<b>RQR. Seguridad</b>	requirement	<p>1. Las soluciones deben dar cumplimiento a las políticas institucionales del sistema de gestión de seguridad de la información establecidas por la entidad que busca garantizar la confidencialidad, integridad y disponibilidad de la información que se genera, procesa, almacena y/o transmite en los sistemas de Información de la Entidad.</p> <p>1. Las soluciones de automatización de procesos a implementar deben permitir la Gestión de Seguridad de Usuarios, grupos de usuarios y asignación de Roles y perfiles de usuarios, permitiendo asociar las acciones disponibles en la solución con respecto a roles de usuario, permitiendo parametrizar las funcionalidades que cada actor puede usar en la solución.</p> <p>1. Un usuario puede estar asociado a uno o más roles, de tal manera que los menús de navegación de la solución se muestran o despliegan dependiendo de</p>	

Name	Type	Description	Properties
		<p>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.</p> <p>1. El diseño de la solución debe definir los criterios necesarios para asegurar la trazabilidad y auditoría sobre las acciones de creación, actualización, modificación o borrado de los componentes de información, de tal manera que la solución debe permitirle al administrador de la solución parametrizar las tablas y eventos que pueden auditarse.</p> <p>1. Las soluciones deben tener en cuenta mecanismos que aseguren el registro histórico para poder mantener la trazabilidad de las acciones realizadas por los usuarios, contemplando el registro de auditoría que contiene información de fecha y hora, identificación del registro, tabla afectada, descripción del evento, tipo de evento, usuario que realiza la acción, identificación de sesión y dirección IP del usuario que efectuó la transacción.</p> <p>1. La solución debe proveer una consulta que permita a un usuario con los privilegios asignados, consultar los registros de auditoría, aplicando criterios de filtro (usuario, maquina, rango de fechas y tipo de operación).</p> <p>1. Las soluciones deben integrarse con LDAP – (Lightweight Directory Access Protocol) para los procesos de inicio de sesión y autenticación. La solución debe soportar la integración Nativa con Active Directory de Microsoft. Para usuarios externos el mecanismo de autorización, autenticación</p>	



Name	Type	Description	Properties
		<p>y acceso será controlado a través del modelo de seguridad de la solución (no habrá autenticación para usuarios externos).</p> <p>1. Las soluciones deben cumplir con los lineamientos de seguridad relacionados a su utilización a través de redes públicas y privadas, garantizando la confidencialidad e integridad de la información y acceso a ella.</p> <p>1. Debe evidenciar que, a través de pruebas de vulnerabilidad, garantiza la seguridad de la información. Estas pruebas deben suministrar evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad.</p> <p>1. Debe incluir un mecanismo de cifrado de los datos que se transportan entre los diferentes componentes tecnológicos y los datos sensibles de la base de datos que representen un alto nivel de confidencialidad.</p> <p>1. A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio).</p> <p>1. Debe contemplar el cumplimiento de la normatividad vigente en cuanto a protección de datos personales y debe permitir el manejo de excepciones.</p> <p>1. Para los casos que aplique se debe permitir el manejo de certificados y/o firmas digitales en los documentos que así se definan para efectos de aprobación y digitalización.</p> <p>1. Debe contemplar las prácticas de desarrollo seguro de aplicaciones y/o implementación segura de productos, para su</p>	

Name	Type	Description	Properties
		<p>naturaleza Web based.</p> <p>1. Debe funcionar sobre protocolo SSL (certificados internos de la entidad cuando los sistemas de información sean internas y certificados validos públicamente cuando los sistemas de información estén expuestas a internet).</p> <p>1. Debe entregar un procedimiento para el respaldo de la información de acuerdo con las necesidades de la entidad.</p> <p>1. Debe incluir uso de criptografía para transacciones y/o campos sensibles según lo indiquen las normas vigentes y las necesidades específicas del negocio de acuerdo como lo determine la entidad.</p> <p>1. Debe contemplar un modelo de datos que garantice base de datos única para evitar que se pueda presentar duplicidad de información.</p> <p>1. En la información confidencial solo puede ser consultada por los perfiles autorizados e igualmente restringir documentos de consulta según los privilegios o permisos asociados.</p> <p>1. A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio).</p> <p>1. Debe cerrar las transacciones luego de máximo 10 minutos de inactividad.</p> <p>1. Debe incluir controles de bloqueo de cuenta después de un máximo de 5 intentos erróneos a fin de evitar ataques de fuerza bruta.</p> <p>1. Debe evidenciar el resultado positivo frente apruebas de ethical hacking, análisis de vulnerabilidades, carga, estrés y desempeño antes de la puesta en operación de acuerdo con los lineamientos de la entidad.</p> <p>1. Debe cumplir con todos</p>	

Name	Type	Description	Properties
		los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la “Guía de desarrollo OWASP” y “OWAS Cheat Sheet”.	

## Lineabase.1a.SIU componentes. infraestructura

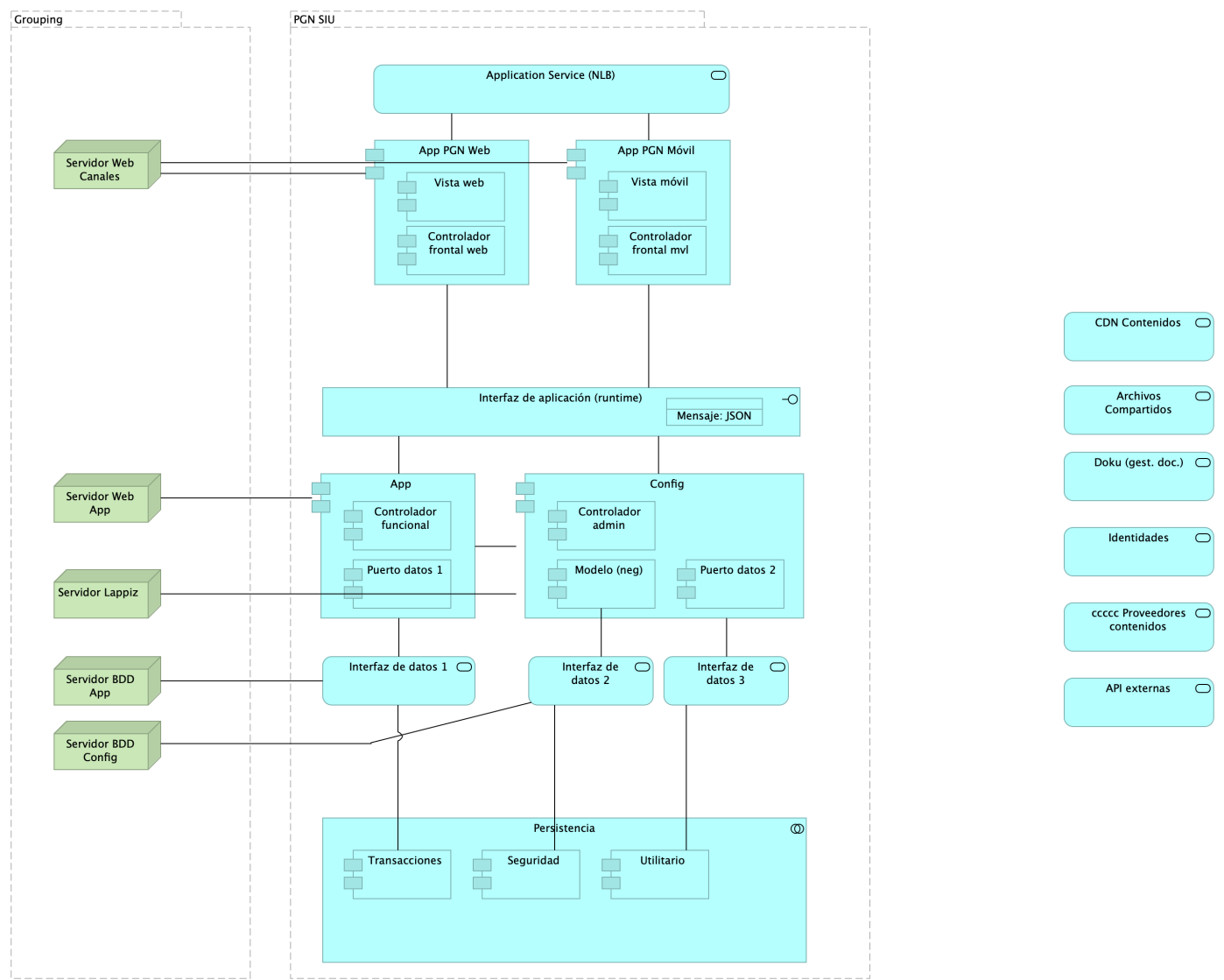


Imagen 3: Diagram: Lineabase.1a.SIU componentes. infraestructura

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

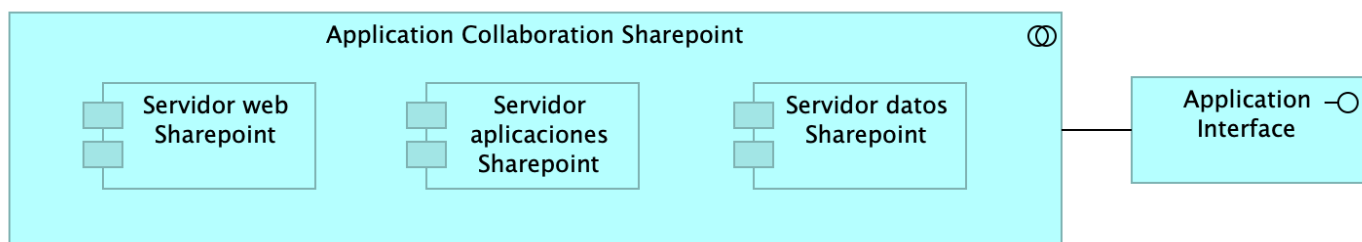
- Servidor de Canales (App PGN web y móvil)
- Servidor Web App (App SUI)
- Servidor Lappiz (Config SUI)
- Servidor BDD App (Transaccional)
- Servidor BDD Config (Configuración)

## Catálogo de Elementos

Name	Type	Description	Properties
Persistencia	application-collaboration		
App	application-component		<i>plataforma: node js</i>
App PGN Móvil	application-component		
App PGN Web	application-component		<i>plataforma: angular 11</i>
Config	application-component		<i>plataforma: cs</i>
Controlador admin	application-component		<i>plataforma: cs</i>
Controlador frontal mvl	application-component		<i>plataforma: js</i>
Controlador frontal web	application-component		<i>plataforma: js</i>
Controlador funcional	application-component		<i>plataforma: js</i>
Modelo (neg)	application-component		<i>plataforma: cs</i>
Puerto datos 1	application-component		<i>plataforma: js</i>
Puerto datos 2	application-component		<i>plataforma: cs</i>
Seguridad	application-component		<i>plataforma: sql</i>
Transacciones	application-component		<i>plataforma: sql</i>
Utilitario	application-component		<i>plataforma: no-sql</i>
Vista móvil	application-component		<i>plataforma: js</i>
Vista web	application-component		<i>plataforma: html</i>
Interfaz de aplicación (runtime)	application-interface		<i>plataforma: angular 11</i>
API externas	application-service		
Application Service (NLB)	application-service		<i>plataforma: angular 11</i>
Archivos Compartidos	application-service		
CDN Contenidos	application-service		
Doku (gest. doc.)	application-service		
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		
Mensaje: JSON	data-object		
Grouping	grouping		

Name	Type	Description	Properties
<b>PGN SIU</b>	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.	
<b>Servidor BDD App</b>	node		
<b>Servidor BDD Config</b>	node		
<b>Servidor Lappiz</b>	node		
<b>Servidor Web App</b>	node		
<b>Servidor Web Canales</b>	node	Nombre físico IP LAN IP Pública	

## Linebase.2.Portal



**Imagen 4:** Diagram: Linebase.2.Portal

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

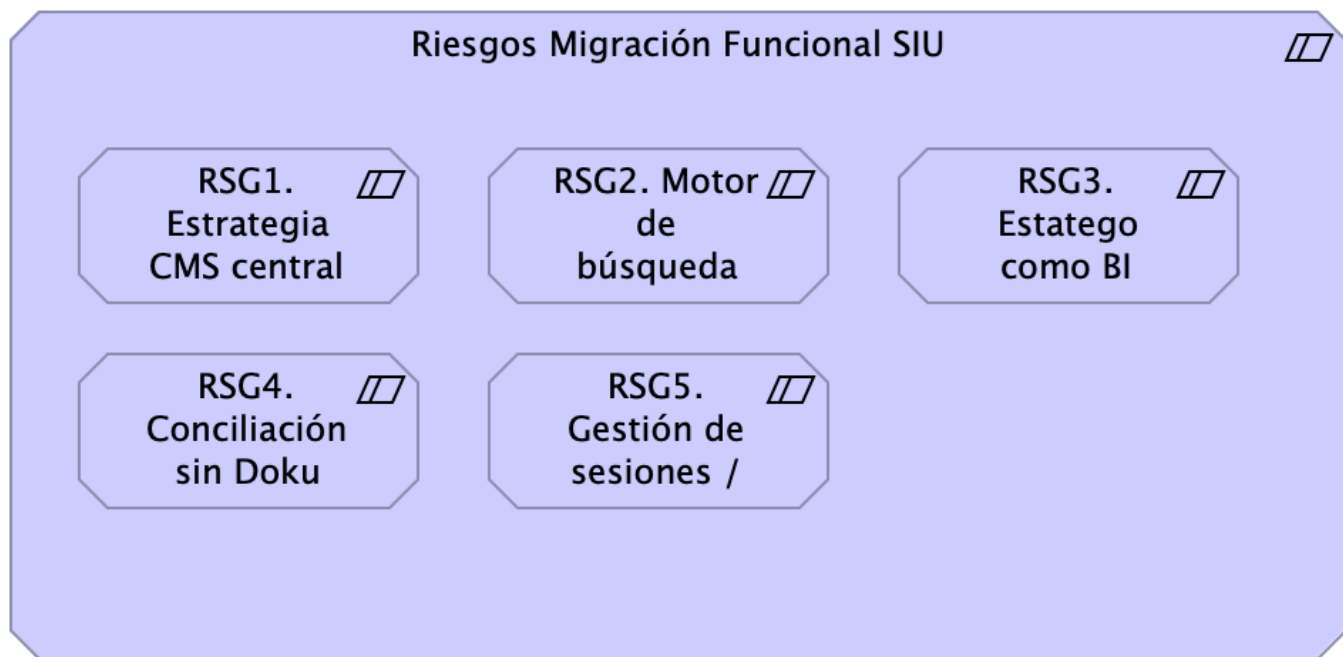
- Servidores Web Front End
- Servidores de Aplicaciones
- Servidores de SQL Server

## Catálogo de Elementos

Name	Type	Description	Properties
<b>Application Collaboration Sharepoint</b>	application-collaboration		

Name	Type	Description	Properties
Servidor aplicaciones Sharepoint	application-component		
Servidor datos Sharepoint	application-component		
Servidor web Sharepoint	application-component		
Application Interface	application-interface		

## 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

### Acciones de Mitigación

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.

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.

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.

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.

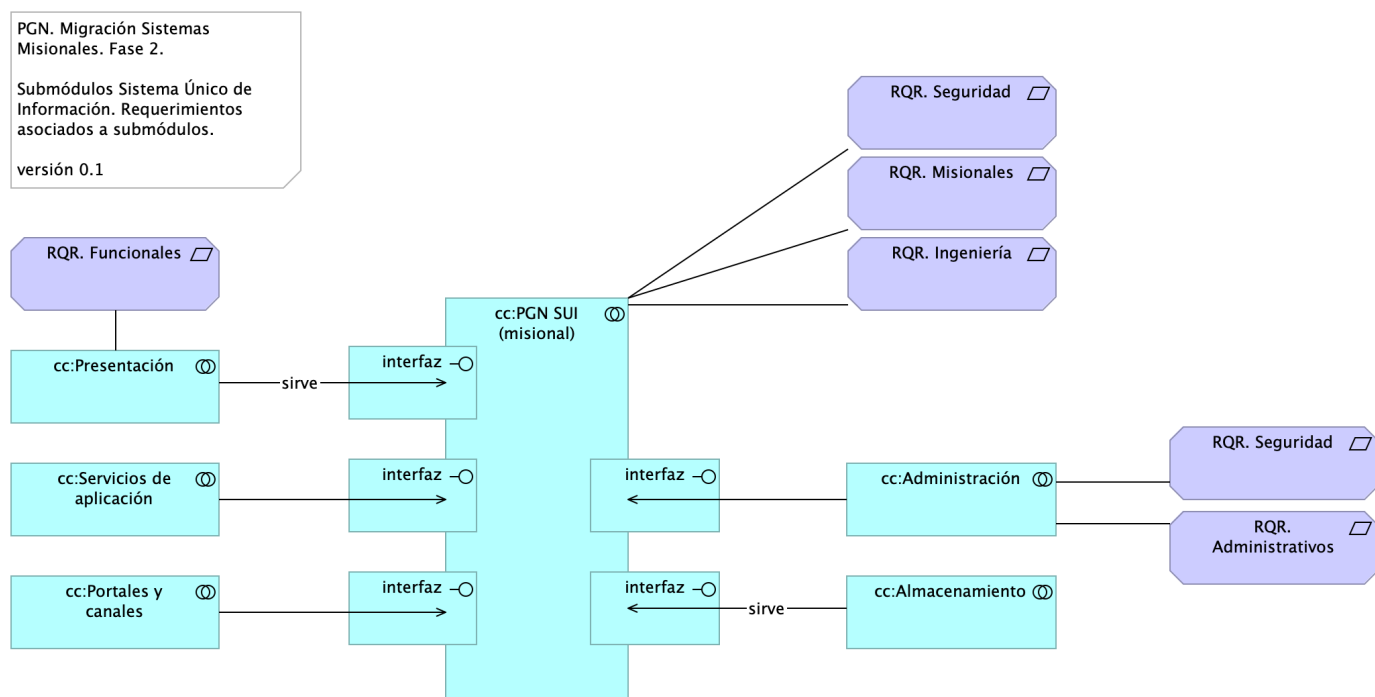
Informar a la PGN de las implicaciones junto con alternativas para la implementación de la acción de manejo del riesgo: facilitar la administración de seguridad en un solo lugar (distinto de localizarla en las aplicaciones web). La PGN debe decidir si o no a la acción propuesta.

## Catálogo de Elementos

Name	Type	Description	Properties
<b>RSG1. Estrategia CMS central</b>	constraint	Establecer desde el principio el gestor de contenidos compartido que los módulos del SUI migrados van a usar.	
<b>RSG2. Motor de búsqueda compartido</b>	constraint	Establecer desde el principio el motor de búsqueda de conteidos compartido para los módulos del SUI migrados.	
<b>RSG3. Estrategio como BI</b>	constraint	Definir la arquitectura de Estrategio migrado: puede ser una solución de BI simple, o puede ser una aplicación web tradicional.	
<b>RSG4. Conciliación sin Doku</b>	constraint	Definir la ubicación de los componentes misionales de Conciliación Administrativa (SIU). Debe estar fuera de Doku.	
<b>RSG5. Gestión de sesiones / caducidad</b>	constraint	Establecer desde el principio el motor de búsqueda de conteidos compartido para los módulos del SUI migrados.	
<b>Riesgos Migración Funcional SIU</b>	constraint		

# Arquitectura Migración PGN SIU

## Migracion.1a.SIU submodulos



**Imagen 6:** Diagram: Migracion.1a.SIU submodulos

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

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

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

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

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

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

## Requerimientos Asociados a los Submódulos

La disposición de los módulos y submódulos presentada, denominada SUI Migración en adelante, facilita la focalización de los requerimientos encontrados en el levantamiento realizado por el actual



proyecto. Así, por ejemplo, los requerimientos funcionales se encuentran concentrados en el submódulo de presentación (ver imagen).

## Catálogo de Elementos

Name	Type	Description	Properties
<b>cc:Administración</b>	application-collaboration		
<b>cc:Almacenamiento</b>	application-collaboration		
<b>cc:PGN SUI (misional)</b>	application-collaboration		
<b>cc:Portales y canales</b>	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.	
<b>cc:Presentación</b>	application-collaboration	Submódulo de presentación del SUI. interfaz gráfica, interfaz web visible a los usuarios clientes y funcionarios de la PGN.	
<b>cc:Servicios de aplicación</b>	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.	
<b>interfaz</b>	application-interface		
<b>interfaz</b>	application-interface		
<b>interfaz</b>	application-interface		
<b>interfaz</b>	application-interface		
<b>interfaz</b>	application-interface		
<b>RQR. Administrativos</b>	requirement		
<b>RQR. Funcionales</b>	requirement		
<b>RQR. Ingeniería</b>	requirement		
<b>RQR. Misionales</b>	requirement		
<b>RQR. Seguridad</b>	requirement	1. Las soluciones deben dar cumplimiento a las políticas institucionales del sistema de gestión de seguridad de la información establecidas por la entidad que busca garantizar la	

Name	Type	Description	Properties
		<p>confidencialidad, integridad y disponibilidad de la información que se genera, procesa, almacena y/o transmite en los sistemas de Información de la Entidad.</p> <p>1. Las soluciones de automatización de procesos a implementar deben permitir la Gestión de Seguridad de Usuarios, grupos de usuarios y asignación de Roles y perfiles de usuarios, permitiendo asociar las acciones disponibles en la solución con respecto a roles de usuario, permitiendo parametrizar las funcionalidades que cada actor puede usar en la solución.</p> <p>1. Un usuario puede estar asociado a uno o más roles, de tal manera que los menús de navegación de la solución se muestran o despliegan dependiendo de las acciones asociadas a cada rol de usuario, permitiendo así que cuando el usuario es autenticado correctamente, la solución verifica los roles que tiene activos para otorgarle únicamente las acciones autorizadas.</p> <p>1. El diseño de la solución debe definir los criterios necesarios para asegurar la trazabilidad y auditoría sobre las acciones de creación, actualización, modificación o borrado de los componentes de información, de tal manera que la solución debe permitirle al administrador de la solución parametrizar las tablas y eventos que pueden auditarse.</p> <p>1. Las soluciones deben tener en cuenta mecanismos que aseguren el registro histórico para poder mantener la trazabilidad de las acciones realizadas por los usuarios, contemplando el registro de auditoría que contiene información de fecha y</p>	

Name	Type	Description	Properties
		<p>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.</p> <p>1. La solución debe proveer una consulta que permita a un usuario con los privilegios asignados, consultar los registros de auditoría, aplicando criterios de filtro (usuario, maquina, rango de fechas y tipo de operación).</p> <p>1. Las soluciones deben integrarse con LDAP – (Lightweight Directory Access Protocol) para los procesos de inicio de sesión y autenticación. La solución debe soportar la integración Nativa con Active Directory de Microsoft. Para usuarios externos el mecanismo de autorización, autenticación y acceso será controlado a través del modelo de seguridad de la solución (no habrá autenticación para usuarios externos).</p> <p>1. Las soluciones deben cumplir con los lineamientos de seguridad relacionados a su utilización a través de redes públicas y privadas, garantizando la confidencialidad e integridad de la información y acceso a ella.</p> <p>1. Debe evidenciar que, a través de pruebas de vulnerabilidad, garantiza la seguridad de la información. Estas pruebas deben suministrar evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad.</p> <p>1. Debe incluir un mecanismo de cifrado de los datos que se transportan entre los diferentes componentes tecnológicos y los datos</p>	

Name	Type	Description	Properties
		<p>sensibles de la base de datos que representen un alto nivel de confidencialidad.</p> <p>1. A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio).</p> <p>1. Debe contemplar el cumplimiento de la normatividad vigente en cuanto a protección de datos personales y debe permitir el manejo de excepciones.</p> <p>1. Para los casos que aplique se debe permitir el manejo de certificados y/o firmas digitales en los documentos que así se definan para efectos de aprobación y digitalización.</p> <p>1. Debe contemplar las prácticas de desarrollo seguro de aplicaciones y/o implementación segura de productos, para su naturaleza Web based.</p> <p>1. Debe funcionar sobre protocolo SSL (certificados internos de la entidad cuando los sistemas de información sean internas y certificados validos públicamente cuando los sistemas de información estén expuestas a internet).</p> <p>1. Debe entregar un procedimiento para el respaldo de la información de acuerdo con las necesidades de la entidad.</p> <p>1. Debe incluir uso de criptografía para transacciones y/o campos sensibles según lo indiquen las normas vigentes y las necesidades específicas del negocio de acuerdo como lo determine la entidad.</p> <p>1. Debe contemplar un modelo de datos que garantice base de datos única para evitar que se pueda presentar duplicidad de información.</p> <p>1. En la información confidencial solo puede ser consultada por los perfiles autorizados e igualmente</p>	

Name	Type	Description	Properties
		<p>restringir documentos de consulta según los privilegios o permisos asociados.</p> <p>1. A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio).</p> <p>1. Debe cerrar las transacciones luego de máximo 10 minutos de inactividad.</p> <p>1. Debe incluir controles de bloqueo de cuenta después de un máximo de 5 intentos erróneos a fin de evitar ataques de fuerza bruta.</p> <p>1. 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.</p> <p>1. Debe cumplir con todos los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la "Guía de desarrollo OWASP" y "OWAS Cheat Sheet".</p>	
RQR. Seguridad	requirement	<p>1. Las soluciones deben dar cumplimiento a las políticas institucionales del sistema de gestión de seguridad de la información establecidas por la entidad que busca garantizar la confidencialidad, integridad y disponibilidad de la información que se genera, procesa, almacena y/o transmite en los sistemas de Información de la Entidad.</p> <p>1. Las soluciones de automatización de procesos a implementar deben permitir la Gestión de Seguridad de Usuarios, grupos de usuarios y asignación de Roles y perfiles de usuarios, permitiendo asociar las acciones disponibles en la solución con respecto a</p>	

Name	Type	Description	Properties
		<p>roles de usuario, permitiendo parametrizar las funcionalidades que cada actor puede usar en la solución.</p> <p>1. Un usuario puede estar asociado a uno o más roles, de tal manera que los menús de navegación de la solución se muestran o despliegan dependiendo de las acciones asociadas a cada rol de usuario, permitiendo así que cuando el usuario es autenticado correctamente, la solución verifica los roles que tiene activos para otorgarle únicamente las acciones autorizadas.</p> <p>1. El diseño de la solución debe definir los criterios necesarios para asegurar la trazabilidad y auditoría sobre las acciones de creación, actualización, modificación o borrado de los componentes de información, de tal manera que la solución debe permitirle al administrador de la solución parametrizar las tablas y eventos que pueden auditarse.</p> <p>1. Las soluciones deben tener en cuenta mecanismos que aseguren el registro histórico para poder mantener la trazabilidad de las acciones realizadas por los usuarios, contemplando el registro de auditoría que contiene información de fecha y hora, identificación del registro, tabla afectada, descripción del evento, tipo de evento, usuario que realiza la acción, identificación de sesión y dirección IP del usuario que efectuó la transacción.</p> <p>1. La solución debe proveer una consulta que permita a un usuario con los privilegios asignados, consultar los registros de auditoría, aplicando criterios de filtro (usuario, maquina, rango de fechas y tipo de operación).</p> <p>1. Las soluciones deben</p>	

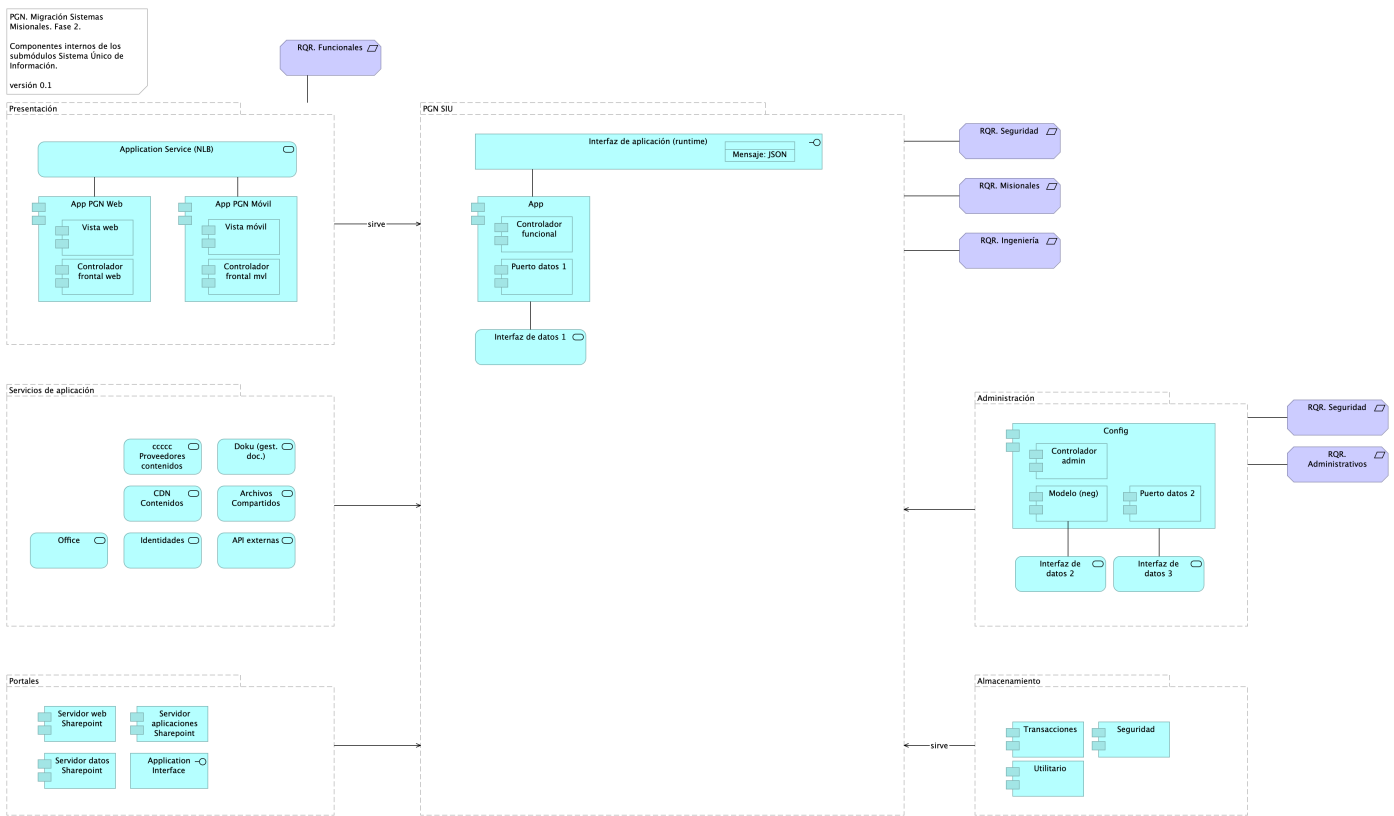
Name	Type	Description	Properties
		<p>integrarse con LDAP – (Lightweight Directory Access Protocol) para los procesos de inicio de sesión y autenticación. La solución debe soportar la integración Nativa con Active Directory de Microsoft. Para usuarios externos el mecanismo de autorización, autenticación y acceso será controlado a través del modelo de seguridad de la solución (no habrá autenticación para usuarios externos).</p> <p>1. Las soluciones deben cumplir con los lineamientos de seguridad relacionados a su utilización a través de redes públicas y privadas, garantizando la confidencialidad e integridad de la información y acceso a ella.</p> <p>1. Debe evidenciar que, a través de pruebas de vulnerabilidad, garantiza la seguridad de la información. Estas pruebas deben suministrar evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad.</p> <p>1. Debe incluir un mecanismo de cifrado de los datos que se transportan entre los diferentes componentes tecnológicos y los datos sensibles de la base de datos que representen un alto nivel de confidencialidad.</p> <p>1. A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio).</p> <p>1. Debe contemplar el cumplimiento de la normatividad vigente en cuanto a protección de datos personales y debe permitir el manejo de excepciones.</p> <p>1. Para los casos que</p>	

Name	Type	Description	Properties
		<p>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.</p> <p>1. Debe contemplar las prácticas de desarrollo seguro de aplicaciones y/o implementación segura de productos, para su naturaleza Web based.</p> <p>1. Debe funcionar sobre protocolo SSL (certificados internos de la entidad cuando los sistemas de información sean internas y certificados validos públicamente cuando los sistemas de información estén expuestas a internet).</p> <p>1. Debe entregar un procedimiento para el respaldo de la información de acuerdo con las necesidades de la entidad.</p> <p>1. Debe incluir uso de criptografía para transacciones y/o campos sensibles según lo indiquen las normas vigentes y las necesidades específicas del negocio de acuerdo como lo determine la entidad.</p> <p>1. Debe contemplar un modelo de datos que garantice base de datos única para evitar que se pueda presentar duplicidad de información.</p> <p>1. En la información confidencial solo puede ser consultada por los perfiles autorizados e igualmente restringir documentos de consulta según los privilegios o permisos asociados.</p> <p>1. A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio).</p> <p>1. Debe cerrar las transacciones luego de máximo 10 minutos de inactividad.</p> <p>1. Debe incluir controles de bloqueo de cuenta después de un máximo de 5 intentos erróneos a fin de evitar</p>	



Name	Type	Description	Properties
		ataques de fuerza bruta. 1. Debe evidenciar el resultado positivo frente apruebas de ethical hacking, análisis de vulnerabilidades, carga, estrés y desempeño antes de la puesta en operación de acuerdo con los lineamientos de la entidad. 1. Debe cumplir con todos los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la “Guía de desarrollo OWASP” y “OWAS Cheat Sheet”.	

## Migracion.1c.SIU submódulos componentes



**Imagen 7:** Diagram: Migracion.1c.SIU submódulos componentes

Presentación de los componentes internos de los submódulos del sistema único de información migración 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 tecnologeias. Los componentes internos y tecnologías elegidas son las siguientes

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

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

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

## Catálogo de Elementos

Name	Type	Description	Properties
<b>App</b>	application-component		<i>plataforma: node js</i>
<b>App PGN Móvil</b>	application-component		
<b>App PGN Web</b>	application-component		<i>plataforma: angular 11</i>
<b>Config</b>	application-component		<i>plataforma: cs</i>
<b>Controlador admin</b>	application-component		<i>plataforma: cs</i>
<b>Controlador frontal mvl</b>	application-component		<i>plataforma: js</i>
<b>Controlador frontal web</b>	application-component		<i>plataforma: js</i>
<b>Controlador funcional</b>	application-component		<i>plataforma: js</i>
<b>Modelo (neg)</b>	application-component		<i>plataforma: cs</i>
<b>Puerto datos 1</b>	application-component		<i>plataforma: js</i>
<b>Puerto datos 2</b>	application-component		<i>plataforma: cs</i>
<b>Seguridad</b>	application-component		<i>plataforma: sql</i>
<b>Servidor aplicaciones Sharepoint</b>	application-component		
<b>Servidor datos Sharepoint</b>	application-component		
<b>Servidor web Sharepoint</b>	application-component		
<b>Transacciones</b>	application-component		<i>plataforma: sql</i>
<b>Utilitario</b>	application-component		<i>plataforma: no-sql</i>
<b>Vista móvil</b>	application-component		<i>plataforma: js</i>
<b>Vista web</b>	application-component		<i>plataforma: html</i>
<b>Application Interface</b>	application-interface		
<b>Interfaz de aplicación (runtime)</b>	application-interface		<i>plataforma: angular 11</i>
<b>API externas</b>	application-service		
<b>Application Service (NLB)</b>	application-service		<i>plataforma: angular 11</i>
<b>Archivos Compartidos</b>	application-service		
<b>CDN Contenidos</b>	application-service		

Name	Type	Description	Properties
<b>Doku (gest. doc.)</b>	application-service		
<b>Identidades</b>	application-service		
<b>Interfaz de datos 1</b>	application-service		
<b>Interfaz de datos 2</b>	application-service		
<b>Interfaz de datos 3</b>	application-service		
<b>Office</b>	application-service		
<b>cccc Proveedores contenidos</b>	application-service		
<b>Mensaje: JSON</b>	data-object		
<b>Administración</b>	grouping		
<b>Almacenamiento</b>	grouping		
<b>PGN SIU</b>	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.	
<b>Portales</b>	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.	
<b>Presentación</b>	grouping	Submódulo de presentación del SUI. interfaz gráfica, interfaz web visible a los usuarios clientes y funcionarios de la PGN.	

Name	Type	Description	Properties
<b>Servicios de aplicación</b>	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.	
<b>RQR. Administrativos</b>	requirement		
<b>RQR. Funcionales</b>	requirement		
<b>RQR. Ingeniería</b>	requirement		
<b>RQR. Misionales</b>	requirement		
<b>RQR. Seguridad</b>	requirement	<p>1. Las soluciones deben dar cumplimiento a las políticas institucionales del sistema de gestión de seguridad de la información establecidas por la entidad que busca garantizar la confidencialidad, integridad y disponibilidad de la información que se genera, procesa, almacena y/o transmite en los sistemas de Información de la Entidad.</p> <p>1. Las soluciones de automatización de procesos a implementar deben permitir la Gestión de Seguridad de Usuarios, grupos de usuarios y asignación de Roles y perfiles de usuarios, permitiendo asociar las acciones disponibles en la solución con respecto a roles de usuario, permitiendo parametrizar las funcionalidades que cada actor puede usar en la solución.</p> <p>1. Un usuario puede estar asociado a uno o más roles, de tal manera que los menús de navegación de la solución se muestran o despliegan dependiendo de las acciones asociadas a cada rol de usuario, permitiendo así que cuando el usuario es autenticado correctamente, la solución verifica los roles que tiene activos para otorgarle</p>	

Name	Type	Description	Properties
		<p>únicamente las acciones autorizadas.</p> <p>1. El diseño de la solución debe definir los criterios necesarios para asegurar la trazabilidad y auditoría sobre las acciones de creación, actualización, modificación o borrado de los componentes de información, de tal manera que la solución debe permitirle al administrador de la solución parametrizar las tablas y eventos que pueden auditarse.</p> <p>1. Las soluciones deben tener en cuenta mecanismos que aseguren el registro histórico para poder mantener la trazabilidad de las acciones realizadas por los usuarios, contemplando el registro de auditoría que contiene información de fecha y hora, identificación del registro, tabla afectada, descripción del evento, tipo de evento, usuario que realiza la acción, identificación de sesión y dirección IP del usuario que efectuó la transacción.</p> <p>1. La solución debe proveer una consulta que permita a un usuario con los privilegios asignados, consultar los registros de auditoría, aplicando criterios de filtro (usuario, maquina, rango de fechas y tipo de operación).</p> <p>1. Las soluciones deben integrarse con LDAP – (Lightweight Directory Access Protocol) para los procesos de inicio de sesión y autenticación. La solución debe soportar la integración Nativa con Active Directory de Microsoft. Para usuarios externos el mecanismo de autorización, autenticación y acceso será controlado a través del modelo de seguridad de la solución (no habrá autenticación para usuarios externos).</p> <p>1. Las soluciones deben cumplir con los</p>	

Name	Type	Description	Properties
		<p>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.</p> <p>1. Debe evidenciar que, a través de pruebas de vulnerabilidad, garantiza la seguridad de la información. Estas pruebas deben suministrar evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad.</p> <p>1. Debe incluir un mecanismo de cifrado de los datos que se transportan entre los diferentes componentes tecnológicos y los datos sensibles de la base de datos que representen un alto nivel de confidencialidad.</p> <p>1. A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio).</p> <p>1. Debe contemplar el cumplimiento de la normatividad vigente en cuanto a protección de datos personales y debe permitir el manejo de excepciones.</p> <p>1. Para los casos que aplique se debe permitir el manejo de certificados y/o firmas digitales en los documentos que así se definan para efectos de aprobación y digitalización.</p> <p>1. Debe contemplar las prácticas de desarrollo seguro de aplicaciones y/o implementación segura de productos, para su naturaleza Web based.</p> <p>1. Debe funcionar sobre protocolo SSL (certificados internos de la entidad cuando los sistemas de información sean internas y certificados validos</p>	

Name	Type	Description	Properties
		<p>públicamente cuando los sistemas de información estén expuestas a internet).</p> <p>1. Debe entregar un procedimiento para el respaldo de la información de acuerdo con las necesidades de la entidad.</p> <p>1. Debe incluir uso de criptografía para transacciones y/o campos sensibles según lo indiquen las normas vigentes y las necesidades específicas del negocio de acuerdo como lo determine la entidad.</p> <p>1. Debe contemplar un modelo de datos que garantice base de datos única para evitar que se pueda presentar duplicidad de información.</p> <p>1. En la información confidencial solo puede ser consultada por los perfiles autorizados e igualmente restringir documentos de consulta según los privilegios o permisos asociados.</p> <p>1. A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio).</p> <p>1. Debe cerrar las transacciones luego de máximo 10 minutos de inactividad.</p> <p>1. Debe incluir controles de bloqueo de cuenta después de un máximo de 5 intentos erróneos a fin de evitar ataques de fuerza bruta.</p> <p>1. 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.</p> <p>1. Debe cumplir con todos los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la "Guía de desarrollo OWASP" y "OWAS Cheat Sheet".</p>	

Name	Requirement type	Description	Properties
RR-001 Seguridad		<p>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.</p> <p>1. Las soluciones de automatización de procesos a implementar deben permitir la Gestión de Seguridad de Usuarios, grupos de usuarios y asignación de Roles y perfiles de usuarios, permitiendo asociar las acciones disponibles en la solución con respecto a roles de usuario, permitiendo parametrizar las funcionalidades que cada actor puede usar en la solución.</p> <p>1. Un usuario puede estar asociado a uno o más roles, de tal manera que los menús de navegación de la solución se muestran o despliegan dependiendo de las acciones asociadas a cada rol de usuario, permitiendo así que cuando el usuario es autenticado correctamente, la solución verifica los roles que tiene activos para otorgarle únicamente las acciones autorizadas.</p> <p>1. El diseño de la solución debe definir los criterios necesarios para asegurar la trazabilidad y auditoría sobre las acciones de creación, actualización, modificación o borrado de los componentes de información, de tal manera que la solución debe permitirle al administrador de la solución parametrizar las tablas y eventos que pueden auditarse.</p> <p>1. Las soluciones deben tener en cuenta mecanismos que aseguren el registro histórico para</p>	



Name	Type	Description	Properties
		<p>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.</p> <p>1. La solución debe proveer una consulta que permita a un usuario con los privilegios asignados, consultar los registros de auditoría, aplicando criterios de filtro (usuario, maquina, rango de fechas y tipo de operación).</p> <p>1. Las soluciones deben integrarse con LDAP – (Lightweight Directory Access Protocol) para los procesos de inicio de sesión y autenticación. La solución debe soportar la integración Nativa con Active Directory de Microsoft. Para usuarios externos el mecanismo de autorización, autenticación y acceso será controlado a través del modelo de seguridad de la solución (no habrá autenticación para usuarios externos).</p> <p>1. Las soluciones deben cumplir con los lineamientos de seguridad relacionados a su utilización a través de redes públicas y privadas, garantizando la confidencialidad e integridad de la información y acceso a ella.</p> <p>1. Debe evidenciar que, a través de pruebas de vulnerabilidad, garantiza la seguridad de la información. Estas pruebas deben suministrar evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad.</p>	

Name	Type	Description	Properties
		<p>1. Debe incluir un mecanismo de cifrado de los datos que se transportan entre los diferentes componentes tecnológicos y los datos sensibles de la base de datos que representen un alto nivel de confidencialidad.</p> <p>1. A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio).</p> <p>1. Debe contemplar el cumplimiento de la normatividad vigente en cuanto a protección de datos personales y debe permitir el manejo de excepciones.</p> <p>1. Para los casos que aplique se debe permitir el manejo de certificados y/o firmas digitales en los documentos que así se definan para efectos de aprobación y digitalización.</p> <p>1. Debe contemplar las prácticas de desarrollo seguro de aplicaciones y/o implementación segura de productos, para su naturaleza Web based.</p> <p>1. Debe funcionar sobre protocolo SSL (certificados internos de la entidad cuando los sistemas de información sean internas y certificados validos públicamente cuando los sistemas de información estén expuestas a internet).</p> <p>1. Debe entregar un procedimiento para el respaldo de la información de acuerdo con las necesidades de la entidad.</p> <p>1. Debe incluir uso de criptografía para transacciones y/o campos sensibles según lo indiquen las normas vigentes y las necesidades específicas del negocio de acuerdo como lo determine la entidad.</p> <p>1. Debe contemplar un modelo de datos que garantice base de datos única para evitar que se</p>	

Name	Type	Description	Properties
		<p>pueda presentar duplicidad de información.</p> <p>1. En la información confidencial solo puede ser consultada por los perfiles autorizados e igualmente restringir documentos de consulta según los privilegios o permisos asociados.</p> <p>1. A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio).</p> <p>1. Debe cerrar las transacciones luego de máximo 10 minutos de inactividad.</p> <p>1. Debe incluir controles de bloqueo de cuenta después de un máximo de 5 intentos erróneos a fin de evitar ataques de fuerza bruta.</p> <p>1. 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.</p> <p>1. Debe cumplir con todos los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la "Guía de desarrollo OWASP" y "OWAS Cheat Sheet".</p>	

## Migracion.1b.SIU submodulos colaboración

---

PGN. Migración Sistemas Misionales. Fase 2.

Patrón de comunicación y colaboración módulo misional (PGN SUI) y submódulos.

versión 0.3

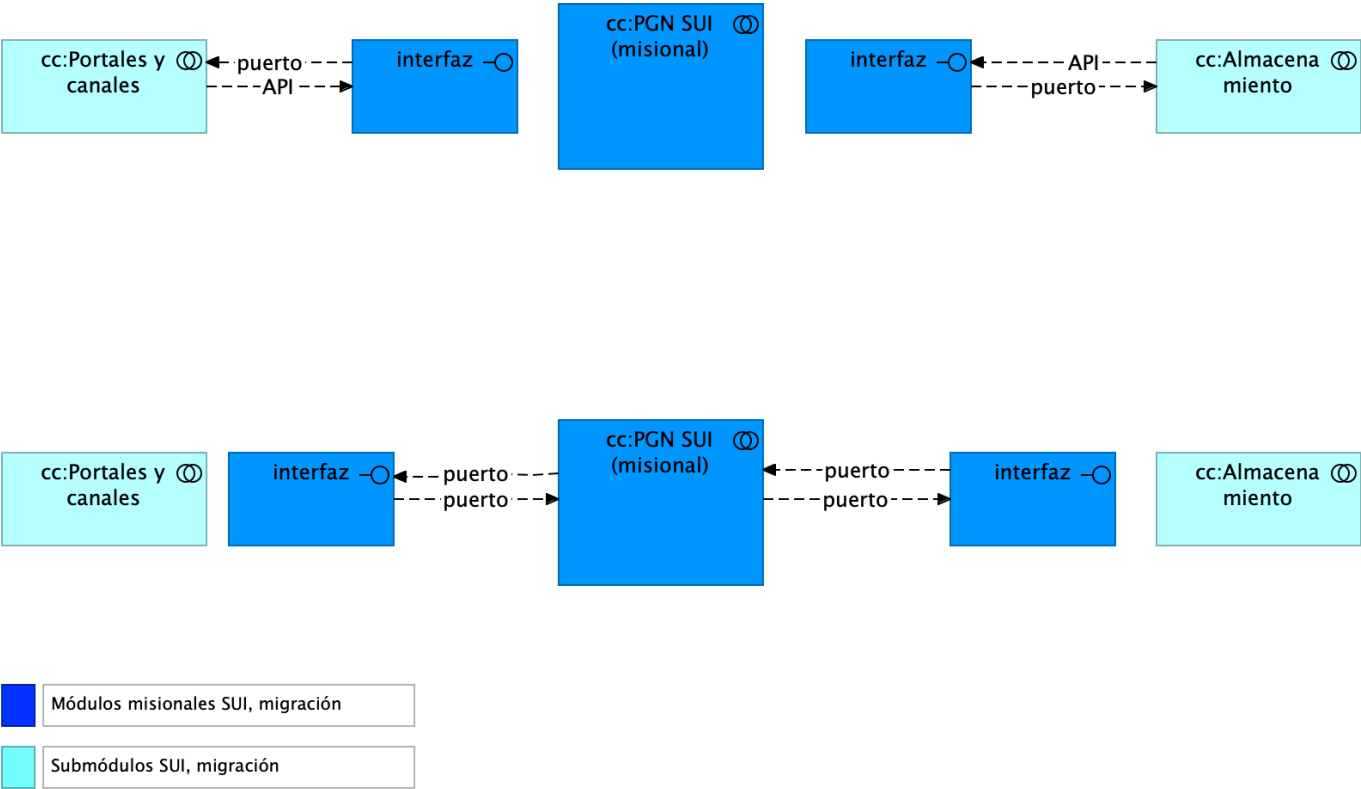


Imagen 8: Diagram: Migracion.1b.SIU submodulos colaboración

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 buses de datos empresarial, sin perjuicio del patrón de comunicación estadar descrito en el diagrama.

### Catálogo de Elementos

Name	Type	Description	Properties
cc:Almacenamiento	application-collaboration		
cc:Almacenamiento	application-collaboration		
cc:PGN SUI (misional)	application-collaboration		
cc:PGN SUI (misional)	application-collaboration		

Name	Type	Description	Properties
<b>cc:Portales y canales</b>	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.	
<b>cc:Portales y canales</b>	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.	
<b>interfaz</b>	application-interface		
<b>interfaz</b>	application-interface		
<b>interfaz</b>	application-interface		
<b>interfaz</b>	application-interface		

# Organización cambios arquitectura

## Organización. 1n. Mapa producto

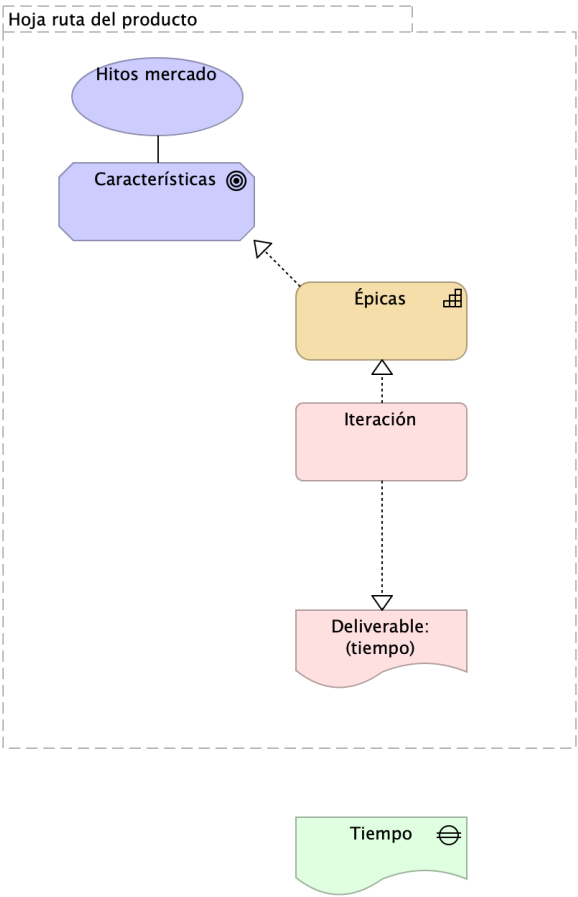
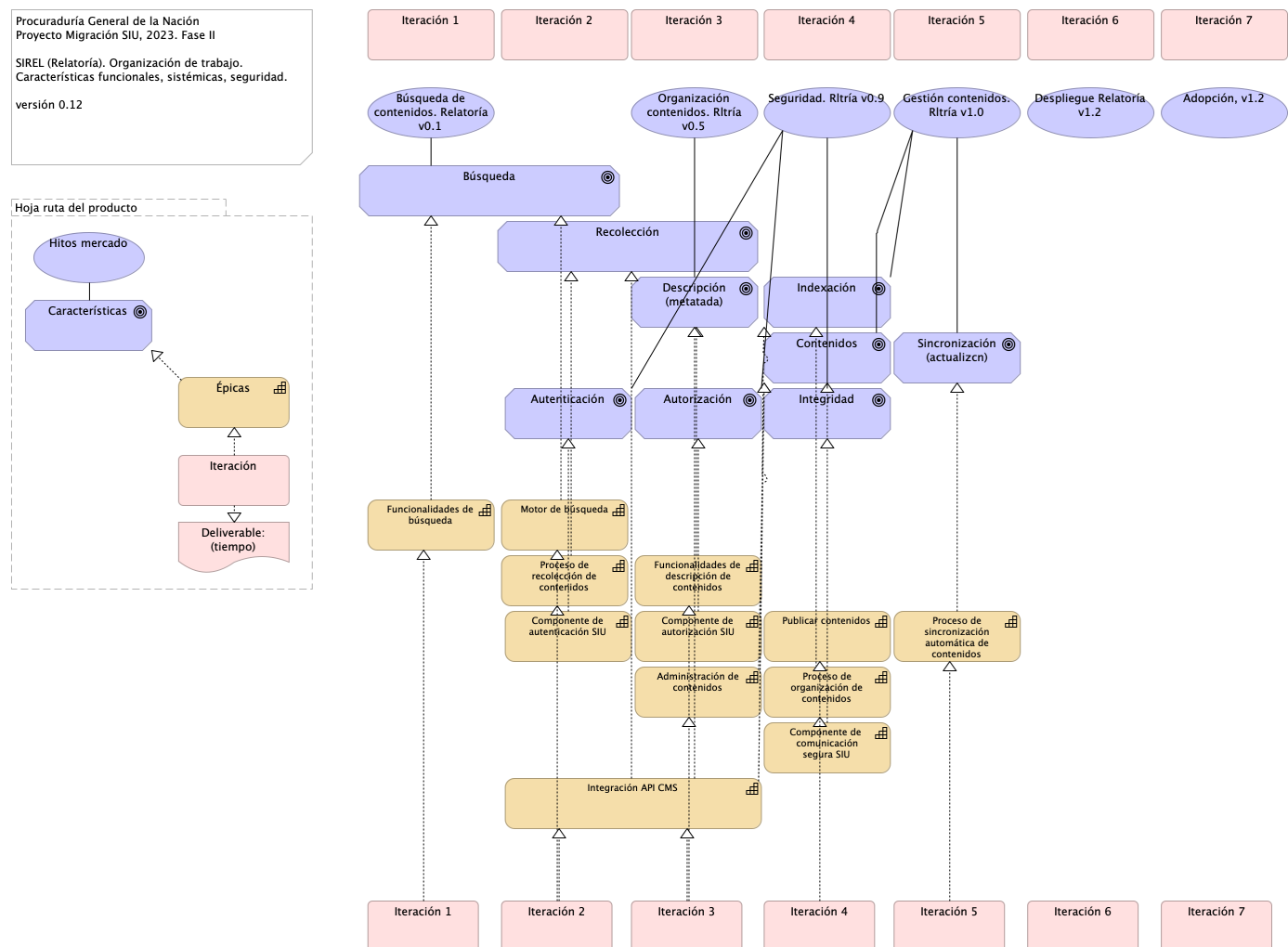


Imagen 9: Diagram: Organización. 1n. Mapa producto

### Catálogo de Elementos

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

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



**Imagen 10:** Diagram: Organización. 1n.1. Mapa producto PGN. Relatoría

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

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

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

## Catálogo de Elementos

Name	Type	Description	Properties
Administración de contenidos	capability		<i>modulo: relatoria</i>
Componente de comunicación segura SIU	capability		<i>modulo: relatoria</i>

Name	Type	Description	Properties
Componente de autenticación SIU	capability		<i>modulo: relatoria</i>
Componente de autorización SIU	capability		<i>modulo: relatoria</i>
Funcionalidades de búsqueda	capability		<i>modulo: relatoria</i>
Funcionalidades de descripción de contenidos	capability		<i>modulo: relatoria</i>
Integración API CMS	capability		<i>modulo: relatoria</i>
Motor de búsqueda	capability		<i>modulo: relatoria</i>
Proceso de organización de contenidos	capability		<i>modulo: relatoria</i>
Proceso de recolección de contenidos	capability		<i>modulo: relatoria</i>
Proceso de sincronización automática de contenidos	capability		<i>modulo: relatoria</i>
Publicar contenidos	capability		<i>modulo: relatoria</i>
Épicas	capability		<i>modulo: relatoria</i>
Deliverable: (tiempo)	deliverable		<i>modulo: relatoria</i>
Autenticación	goal		<i>modulo: relatoria</i> <i>característica: seguridad</i>
Autorización	goal		<i>modulo: relatoria</i> <i>característica: seguridad</i>
Búsqueda	goal		<i>modulo: relatoria</i> <i>característica: técnica, integración</i>
Características	goal		<i>modulo: relatoria</i>
Contenidos	goal		<i>modulo: relatoria</i> <i>característica: técnica, integración</i>
Descripción (metatada)	goal		<i>modulo: relatoria</i> <i>característica: técnica, integración</i>
Indexación	goal		<i>modulo: relatoria</i> <i>característica: técnica, integración</i>
Integridad	goal		<i>modulo: relatoria</i> <i>característica: seguridad</i>
Recolección	goal		<i>modulo: relatoria</i> <i>característica: técnica, integración</i>
Sincronización (actualizcn)	goal		<i>modulo: relatoria</i> <i>característica: técnica, integración</i>
Hoja ruta del producto	grouping		<i>modulo: relatoria</i>



Name	Type	Description	Properties
Adopción, v1.2	value		<i>modulo: relatoria</i>
Búsqueda de contenidos. Relatoria v0.1	value		<i>modulo: relatoria</i>
Despliegue Relatoria v1.2	value		<i>modulo: relatoria</i>
Gestión contenidos. Rltria v1.0	value		<i>modulo: relatoria</i>
Hitos mercado	value		<i>modulo: relatoria</i>
Organización contenidos. Rltria v0.5	value		<i>modulo: relatoria</i>
Seguridad. Rltria v0.9	value		<i>modulo: relatoria</i>
Iteración	work-package		<i>modulo: relatoria</i>
Iteración 1	work-package		<i>modulo: relatoria</i>
Iteración 1	work-package		<i>modulo: relatoria</i>
Iteración 2	work-package		<i>modulo: relatoria</i>
Iteración 2	work-package		<i>modulo: relatoria</i>
Iteración 3	work-package		<i>modulo: relatoria</i>
Iteración 3	work-package		<i>modulo: relatoria</i>
Iteración 4	work-package		<i>modulo: relatoria</i>
Iteración 4	work-package		<i>modulo: relatoria</i>
Iteración 5	work-package		<i>modulo: relatoria</i>
Iteración 5	work-package		<i>modulo: relatoria</i>
Iteración 6	work-package		<i>modulo: relatoria</i>
Iteración 6	work-package		<i>modulo: relatoria</i>
Iteración 7	work-package		<i>modulo: relatoria</i>
Iteración 7	work-package		<i>modulo: relatoria</i>

# Arquitectura de Seguridad, SUI Migración

## Seguridad. 1. Requerimientos

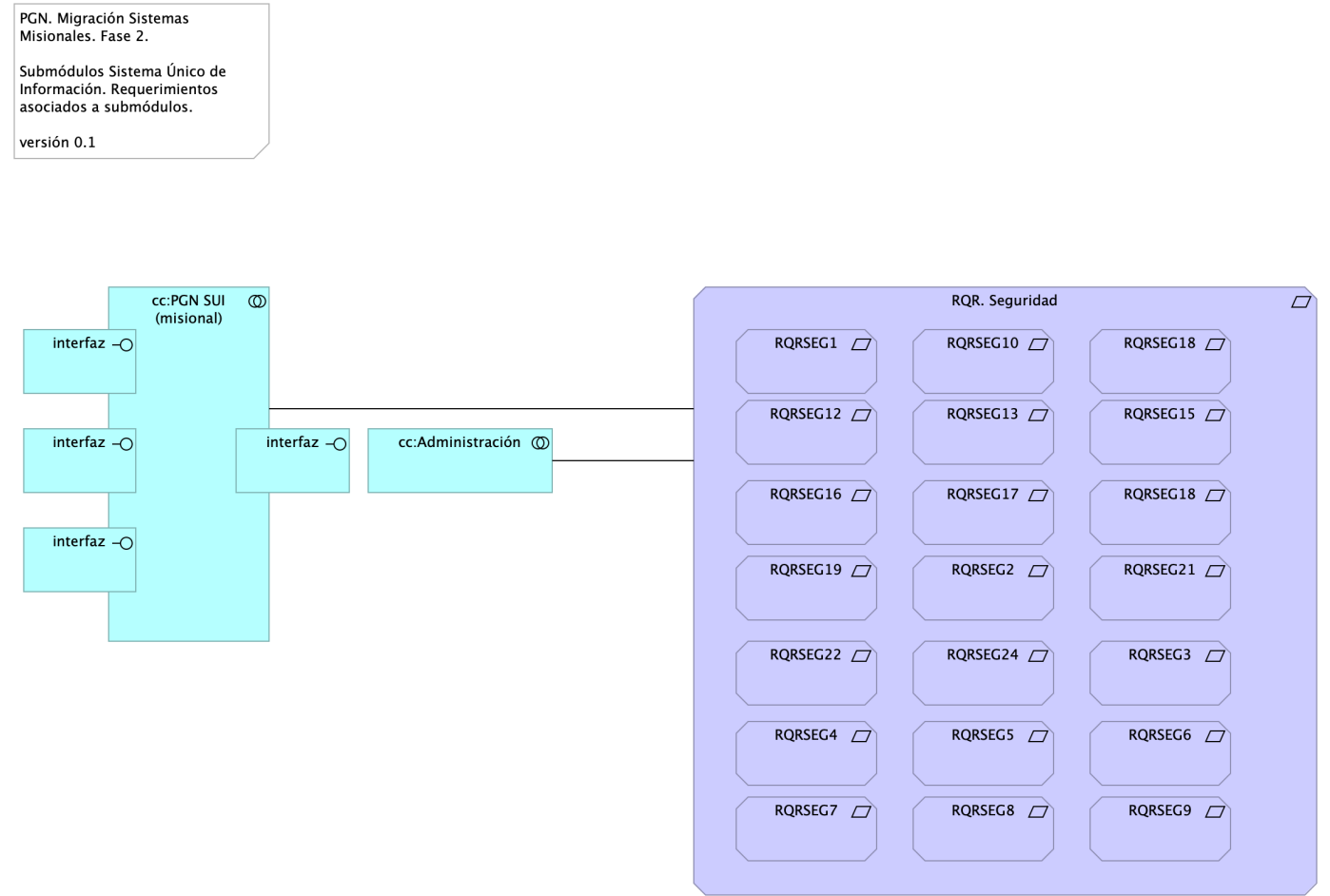


Imagen 11: Diagram: Seguridad. 1. Requerimientos

### Catálogo de Elementos

Name	Type	Description	Properties
cc:Administración	application-collaboration		
cc:PGN SUI (misional)	application-collaboration		
interfaz	application-interface		
interfaz	application-interface		
interfaz	application-interface		
interfaz	application-interface		
RQR. Seguridad	requirement	1. Las soluciones deben dar cumplimiento a las políticas institucionales del sistema de gestión de seguridad de la información establecidas por la entidad que busca garantizar la confidencialidad, integridad	

Name	Type	Description	Properties
		<p>y disponibilidad de la información que se genera, procesa, almacena y/o transmite en los sistemas de Información de la Entidad.</p> <p>1. Las soluciones de automatización de procesos a implementar deben permitir la Gestión de Seguridad de Usuarios, grupos de usuarios y asignación de Roles y perfiles de usuarios, permitiendo asociar las acciones disponibles en la solución con respecto a roles de usuario, permitiendo parametrizar las funcionalidades que cada actor puede usar en la solución.</p> <p>1. Un usuario puede estar asociado a uno o más roles, de tal manera que los menús de navegación de la solución se muestran o despliegan dependiendo de las acciones asociadas a cada rol de usuario, permitiendo así que cuando el usuario es autenticado correctamente, la solución verifica los roles que tiene activos para otorgarle únicamente las acciones autorizadas.</p> <p>1. El diseño de la solución debe definir los criterios necesarios para asegurar la trazabilidad y auditoría sobre las acciones de creación, actualización, modificación o borrado de los componentes de información, de tal manera que la solución debe permitirle al administrador de la solución parametrizar las tablas y eventos que pueden auditarse.</p> <p>1. Las soluciones deben tener en cuenta mecanismos que aseguren el registro histórico para poder mantener la trazabilidad de las acciones realizadas por los usuarios, contemplando el registro de auditoría que contiene información de fecha y hora, identificación del</p>	

Name	Type	Description	Properties
		<p>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.</p> <p>1. La solución debe proveer una consulta que permita a un usuario con los privilegios asignados, consultar los registros de auditoría, aplicando criterios de filtro (usuario, maquina, rango de fechas y tipo de operación).</p> <p>1. Las soluciones deben integrarse con LDAP – (Lightweight Directory Access Protocol) para los procesos de inicio de sesión y autenticación. La solución debe soportar la integración Nativa con Active Directory de Microsoft. Para usuarios externos el mecanismo de autorización, autenticación y acceso será controlado a través del modelo de seguridad de la solución (no habrá autenticación para usuarios externos).</p> <p>1. Las soluciones deben cumplir con los lineamientos de seguridad relacionados a su utilización a través de redes públicas y privadas, garantizando la confidencialidad e integridad de la información y acceso a ella.</p> <p>1. Debe evidenciar que, a través de pruebas de vulnerabilidad, garantiza la seguridad de la información. Estas pruebas deben suministrar evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad.</p> <p>1. Debe incluir un mecanismo de cifrado de los datos que se transportan entre los diferentes componentes tecnológicos y los datos sensibles de la base de</p>	

Name	Type	Description	Properties
		<p>datos que representen un alto nivel de confidencialidad.</p> <p>1. A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio).</p> <p>1. Debe contemplar el cumplimiento de la normatividad vigente en cuanto a protección de datos personales y debe permitir el manejo de excepciones.</p> <p>1. Para los casos que aplique se debe permitir el manejo de certificados y/o firmas digitales en los documentos que así se definan para efectos de aprobación y digitalización.</p> <p>1. Debe contemplar las prácticas de desarrollo seguro de aplicaciones y/o implementación segura de productos, para su naturaleza Web based.</p> <p>1. Debe funcionar sobre protocolo SSL (certificados internos de la entidad cuando los sistemas de información sean internas y certificados validos públicamente cuando los sistemas de información estén expuestas a internet).</p> <p>1. Debe entregar un procedimiento para el respaldo de la información de acuerdo con las necesidades de la entidad.</p> <p>1. Debe incluir uso de criptografía para transacciones y/o campos sensibles según lo indiquen las normas vigentes y las necesidades específicas del negocio de acuerdo como lo determine la entidad.</p> <p>1. Debe contemplar un modelo de datos que garantice base de datos única para evitar que se pueda presentar duplicidad de información.</p> <p>1. En la información confidencial solo puede ser consultada por los perfiles autorizados e igualmente restringir documentos de</p>	

Name	Type	Description	Properties
		<p>consulta según los privilegios o permisos asociados.</p> <p>1. A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio).</p> <p>1. Debe cerrar las transacciones luego de máximo 10 minutos de inactividad.</p> <p>1. Debe incluir controles de bloqueo de cuenta después de un máximo de 5 intentos erróneos a fin de evitar ataques de fuerza bruta.</p> <p>1. 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.</p> <p>1. Debe cumplir con todos los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la "Guía de desarrollo OWASP" y "OWAS Cheat Sheet".</p>	
<b>RQRSEG1</b>	requirement	<p>1. Las soluciones deben dar cumplimiento a las políticas institucionales del sistema de gestión de seguridad de la información establecidas por la entidad que busca garantizar la confidencialidad, integridad y disponibilidad de la información que se genera, procesa, almacena y/o transmite en los sistemas de Información de la Entidad.</p>	
<b>RQRSEG10</b>	requirement	<p>1. Debe incluir un mecanismo de cifrado de los datos que se transportan entre los diferentes componentes tecnológicos y los datos sensibles de la base de datos que representen un alto nivel de confidencialidad.</p>	

Name	Type	Description	Properties
<b>RQRSEG12</b>	requirement	1. Debe contemplar el cumplimiento de la normatividad vigente en cuanto a protección de datos personales y debe permitir el manejo de excepciones.	
<b>RQRSEG13</b>	requirement	1. Para los casos que aplique se debe permitir el manejo de certificados y/o firmas digitales en los documentos que así se definan para efectos de aprobación y digitalización.	
<b>RQRSEG15</b>	requirement	1. Debe funcionar sobre protocolo SSL (certificados internos de la entidad cuando los sistemas de información sean internas y certificados validos públicamente cuando los sistemas de información estén expuestas a internet).	
<b>RQRSEG16</b>	requirement	1. Debe entregar un procedimiento para el respaldo de la información de acuerdo con las necesidades de la entidad.	
<b>RQRSEG17</b>	requirement	1. Debe incluir uso de criptografía para transacciones y/o campos sensibles según lo indiquen las normas vigentes y las necesidades específicas del negocio de acuerdo como lo determine la entidad.	
<b>RQRSEG18</b>	requirement	"1. Debe contemplar un modelo de datos que garantice base de datos única para evitar que se pueda presentar duplicidad de información."	
<b>RQRSEG18</b>	requirement	1. Debe contemplar un modelo de datos que garantice base de datos única para evitar que se pueda presentar duplicidad de información.,id-d1a6b80e7a6c4538b922f333f4d7ec7a,requirement RQRSEG11,"1. A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio).	

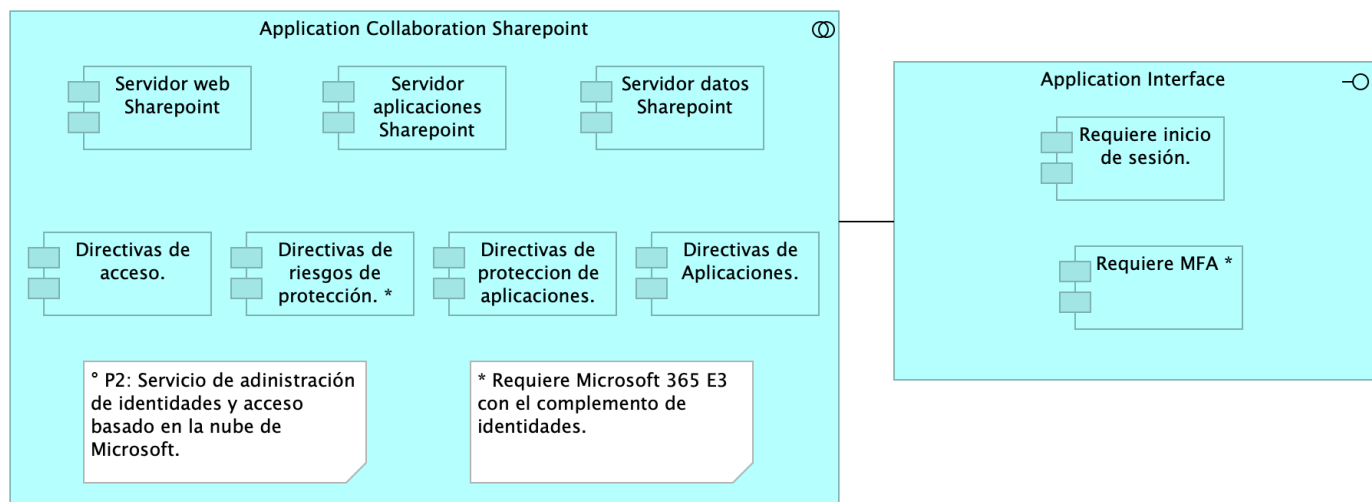
Name	Type	Description	Properties
RQRSEG19	requirement	1. En la información confidencial solo puede ser consultada por los perfiles autorizados e igualmente restringir documentos de consulta según los privilegios o permisos asociados.	
RQRSEG2	requirement	1. Las soluciones de automatización de procesos a implementar deben permitir la Gestión de Seguridad de Usuarios, grupos de usuarios y asignación de Roles y perfiles de usuarios, permitiendo asociar las acciones disponibles en la solución con respecto a roles de usuario, permitiendo parametrizar las funcionalidades que cada actor puede usar en la solución.	
RQRSEG21	requirement	1. Debe cerrar las transacciones luego de máximo 10 minutos de inactividad. ""	
RQRSEG22	requirement	1. Debe incluir controles de bloqueo de cuenta después de un máximo de 5 intentos erróneos a fin de evitar ataques de fuerza bruta.	
RQRSEG24	requirement	1. Debe cumplir con todos los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la "Guía de desarrollo OWASP" y "OWAS Cheat Sheet	
RQRSEG3	requirement	1. Un usuario puede estar asociado a uno o más roles, de tal manera que los menús de navegación de la solución se muestran o despliegan dependiendo de las acciones asociadas a cada rol de usuario, permitiendo así que cuando el usuario es autenticado correctamente, la solución verifica los roles que tiene activos para otorgarle únicamente las acciones autorizadas.	



Name	Type	Description	Properties
<b>RQRSEG4</b>	requirement	1. El diseño de la solución debe definir los criterios necesarios para asegurar la trazabilidad y auditoría sobre las acciones de creación, actualización, modificación o borrado de los componentes de información, de tal manera que la solución debe permitirle al administrador de la solución parametrizar las tablas y eventos que pueden auditarse.	
<b>RQRSEG5</b>	requirement	1. Las soluciones deben tener en cuenta mecanismos que aseguren el registro histórico para poder mantener la trazabilidad de las acciones realizadas por los usuarios, contemplando el registro de auditoría que contiene información de fecha y hora, identificación del registro, tabla afectada, descripción del evento, tipo de evento, usuario que realiza la acción, identificación de sesión y dirección IP del usuario que efectuó la transacción.	
<b>RQRSEG6</b>	requirement	1. La solución debe proveer una consulta que permita a un usuario con los privilegios asignados, consultar los registros de auditoría, aplicando criterios de filtro (usuario, maquina, rango de fechas y tipo de operación).	
<b>RQRSEG7</b>	requirement	1. Las soluciones deben integrarse con LDAP – (Lightweight Directory Access Protocol) para los procesos de inicio de sesión y autenticación. La solución debe soportar la integración Nativa con Active Directory de Microsoft. Para usuarios externos el mecanismo de autorización, autenticación y acceso será controlado a través del modelo de seguridad de la solución (no habrá autenticación para usuarios externos).	

Name	Type	Description	Properties
RQRSEG8	requirement	1. Las soluciones deben cumplir con los lineamientos de seguridad relacionados a su utilización a través de redes públicas y privadas, garantizando la confidencialidad e integridad de la información y acceso a ella.	
RQRSEG9	requirement	1. Debe evidenciar que, a través de pruebas de vulnerabilidad, garantiza la seguridad de la información. Estas pruebas deben suministrar evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad.	

## Seguridad. Linebase.2.Porta



**Imagen 12:** Diagram: Seguridad. Linebase.2.Porta

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

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

## Catálogo de Elementos

Name	Type	Description	Properties
Application Collaboration Sharepoint	application-collaboration		

Name	Type	Description	Properties
Directivas de Aplicaciones.	application-component		
Directivas de acceso.	application-component		
Directivas de proteccion de aplicaciones.	application-component		
Directivas de riesgos de protección. *	application-component		
Requiere MFA *	application-component		
Requiere inicio de sesión.	application-component		
Servidor aplicaciones Sharepoint	application-component		
Servidor datos Sharepoint	application-component		
Servidor web Sharepoint	application-component		
Application Interface	application-interface		

Generated on: Mon Sep 11 2023 13:57:39 GMT-0500 (COT)

## Requerimientos de Administración

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

# Requerimientos de Seguridad

---

1. Las soluciones deben dar cumplimiento a las políticas institucionales del sistema de gestión de seguridad de la información establecidas por la entidad que busca garantizar la confidencialidad, integridad y disponibilidad de la información que se genera, procesa, almacena y/o transmite en los sistemas de Información de la Entidad.
2. Las soluciones de automatización de procesos a implementar deben permitir la Gestión de Seguridad de Usuarios, grupos de usuarios y asignación de Roles y perfiles de usuarios, permitiendo asociar las acciones disponibles en la solución con respecto a roles de usuario, permitiendo parametrizar las funcionalidades que cada actor puede usar en la solución.
3. Un usuario puede estar asociado a uno o más roles, de tal manera que los menús de navegación de la solución se muestran o despliegan dependiendo de las acciones asociadas a cada rol de usuario, permitiendo así que cuando el usuario es autenticado correctamente, la solución verifica los roles que tiene activos para otorgarle únicamente las acciones autorizadas.
4. El diseño de la solución debe definir los criterios necesarios para asegurar la trazabilidad y auditoría sobre las acciones de creación, actualización, modificación o borrado de los componentes de información, de tal manera que la solución debe permitirle al administrador de la solución parametrizar las tablas y eventos que pueden auditarse.
5. Las soluciones deben tener en cuenta mecanismos que aseguren el registro histórico para poder mantener la trazabilidad de las acciones realizadas por los usuarios, contemplando el registro de auditoría que contiene información de fecha y hora, identificación del registro, tabla afectada, descripción del evento, tipo de evento, usuario que realiza la acción, identificación de sesión y dirección IP del usuario que efectuó la transacción.
6. La solución debe proveer una consulta que permita a un usuario con los privilegios asignados, consultar los registros de auditoría, aplicando criterios de filtro (usuario, maquina, rango de fechas y tipo de operación).
7. Las soluciones deben integrarse con LDAP – (Lightweight Directory Access Protocol) para los procesos de inicio de sesión y autenticación. La solución debe soportar la integración Nativa con Active Directory de Microsoft. Para usuarios externos el mecanismo de autorización, autenticación y acceso será controlado a través del modelo de seguridad de la solución (no habrá autenticación para usuarios externos).
8. Las soluciones deben cumplir con los lineamientos de seguridad relacionados a su utilización a través de redes públicas y privadas, garantizando la confidencialidad e integridad de la información y acceso a ella.
9. Debe evidenciar que, a través de pruebas de vulnerabilidad, garantiza la seguridad de la información. Estas pruebas deben suministrar evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad.
10. Debe incluir un mecanismo de cifrado de los datos que se transportan entre los diferentes componentes tecnológicos y los datos sensibles de la base de datos que representen un alto nivel de confidencialidad.
11. A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio).
12. Debe contemplar el cumplimiento de la normatividad vigente en cuanto a protección de datos personales y debe permitir el manejo de excepciones.
13. Para los casos que aplique se debe permitir el manejo de certificados y/o firmas digitales en los documentos que así se definan para efectos de aprobación y digitalización.
14. Debe contemplar las prácticas de desarrollo seguro de aplicaciones y/o implementación segura de productos, para su naturaleza Web based.
15. Debe funcionar sobre protocolo SSL (certificados internos de la entidad cuando los sistemas de información sean internas y certificados validos públicamente cuando los sistemas de información estén expuestas a internet).
16. Debe entregar un procedimiento para el respaldo de la información de acuerdo con las necesidades de la entidad.

17. Debe incluir uso de criptografía para transacciones y/o campos sensibles según lo indiquen las normas vigentes y las necesidades específicas del negocio de acuerdo como lo determine la entidad.
18. Debe contemplar un modelo de datos que garantice base de datos única para evitar que se pueda presentar duplicidad de información.
19. En la información confidencial solo puede ser consultada por los perfiles autorizados e igualmente restringir documentos de consulta según los privilegios o permisos asociados.
20. A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio).
21. Debe cerrar las transacciones luego de máximo 10 minutos de inactividad.
22. Debe incluir controles de bloqueo de cuenta después de un máximo de 5 intentos erróneos a fin de evitar ataques de fuerza bruta.
23. Debe evidenciar el resultado positivo frente 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] [[eservices3-22?](#)] [[eservices4-22?](#)] [[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/>