

# Documento de Arquitectura Migración Funcional PGN SIU

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

**Versión** del producto 1.13c5f29 de 22 Oct 2023

**Presentado a**

Procuraduría General de la Nación (PGN)

**Fecha**

22 Oct 2023

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@13c5f29](mailto:Sharepoint.Softgic@13c5f29) del October 22, 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        |   |
| 1.13c5f29      | 2023-10-22. histr2                                      |
| 1.7e6a6e7      | 2023-10-22. histr1                                      |
| 1.50977db      | 2023-10-19. upd   |
| 1.809e99c      | 2023-09-14. pndc  |
| Vínculos       | <a href="#">N003a Vista Segmento PGN SIU</a>            |

# Contenidos

---

# Introducción

## Propósito

---

Este documento tiene como propósito presentar la arquitectura del aplicativo Sistema Único de Información (SUI) para Procuraduría General de la Nación (PGN). según los requerimientos definidos durante la etapa de preventa y luego detallados en las historias de usuario.

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

La definición arquitectónica de este proyecto será un proceso evolutivo como tal. Este documento puede ser susceptible a cambios a medida que se vayan agregando nuevas funcionalidades o requisitos al sistema.

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

# Restricciones Principales

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

Lista de restricciones de la migración SUI, 2023.

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

## Restricciones Secundarias

---

Otras restricciones a detallar.

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

## Requisitos de Arquitectura (no funcional)

Entendemos como requisitos de arquitectura aquellos requerimientos no visibles pero estructurales, medibles, y que impactan al funcionamiento, desarrollo y mantenimiento de la solución migración SUI, objeto de este proyecto, OP 078-2023.

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

## Requerimientos generales

---

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

# Requisitos de Arquitectura (no funcional) Particulares

## Extensibilidad SUI

**Tabla 1:** Requisito no. 1, 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. |

## Mantenibilidad SUI

**Tabla 2:** Requisito no. 2.

| 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. |

# 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

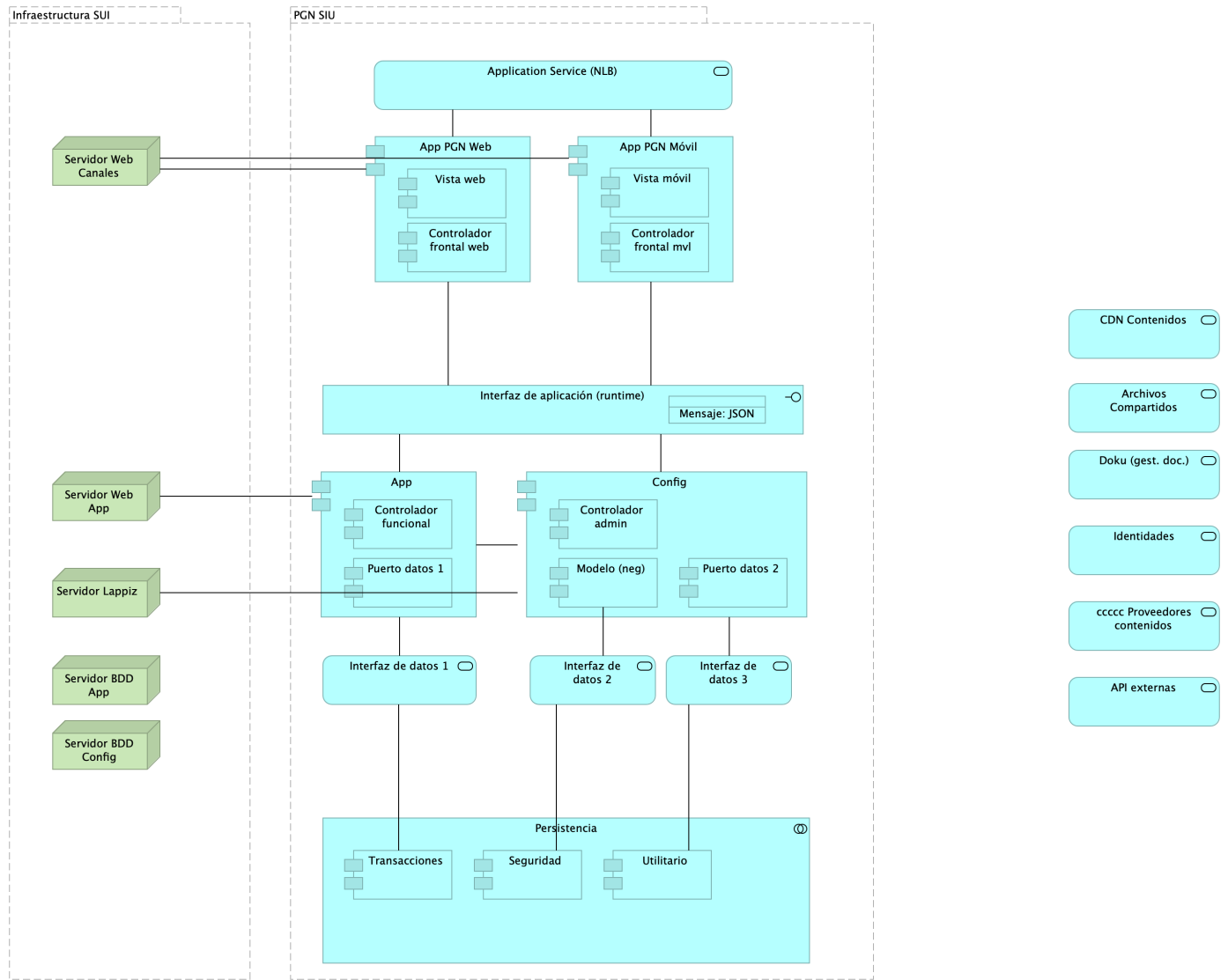


Imagen 1: Diagram: Lineabase.1a.SIU componentes. infraestructura

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 |             |            |

| Name          | Type                  | Description   | Properties  |
|---------------|-----------------------|---|---|
| App           | application-component |   | <i>plataforma:</i> node Js<br><i>brecha:</i> 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. Protección de datos personales, Los sistemas de información que recogen, procesan y almacenan información de los derechos de las personas se deben almacenar de forma adecuada, la información que pueda ser vulnerada puede generar obliaciones legales y éticas con respecto a la perdida de informacion confidencial por parte de ciudadanos del pais. La informacion contenida en las bases de datos debe tener los mecanismos de cifrado que en otros apartados se han mencionado. La legislación que hay que tener como referencia, ley 1581 de 2012. Decreto 1377 de 2013 La metodologia empleada tendrá las siguientes fases:</p> <ul style="list-style-type: none"> <li>• FASE DE RECONOCIMIENTO:<br/>Se recolectará toda la información posible, usando diferentes técnicas como:<br/>o Recopilación de dominios/IPs/puertos/servicios<br/>o Recopilación de metadatos<br/>o Uso de Google Dorks.</li> <li>• ANÁLISIS DE VULNERABILIDADES:<br/>Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.</li> <li>• EXPLOTACIÓN:</li> </ul> | <i>plantilla:</i> element-md-bold<br><i>brecha:</i> 100 |

| Name        | Type                  | Description  | Properties   |
|-------------|-----------------------|--|--|
|             |                       | <ul style="list-style-type: none"> <li>• Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo:               <ul style="list-style-type: none"> <li>o Inyección de código</li> <li>o Inclusión de ficheros locales o remotos</li> <li>o Evasión de autenticación</li> <li>o Carencia de controles de autorización</li> <li>o Ejecución de comandos en el lado del servidor</li> <li>o Ataques tipo Cross Site Request Forgery</li> <li>o Control de errores</li> <li>o Gestión de sesiones</li> <li>o Fugas de información</li> <li>o Secuestros de sesión</li> <li>o Comprobación de las condiciones para realizar una denegación de servicio.</li> </ul> </li> <li>• POST EXPLOTACIÓN:<br/>En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adicionales con el objetivo de comprobar la criticidad de esta.<br/>No URL IP<br/>1.<br/><a href="https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz">https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz</a><br/>135.181.185.207</li> </ul> |  |
| 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"> <li>• FASE DE RECONOCIMIENTO:<br/>Se recolectará toda la información posible, usando diferentes técnicas</li> </ul>   | <p><i>plataforma:</i> angular 11</p> <p><i>brecha:</i> 100</p> |

| Name   | Type                  | Description  | Properties     |
|--------|-----------------------|--|----------------|
|        |                       | <p>como:</p> <ul style="list-style-type: none"> <li>o Recopilación de dominios/IPs/puertos/servicios</li> <li>o Recopilación de metadatos</li> <li>o Uso de Google Dorks.</li> </ul> <p>• ANÁLISIS DE VULNERABILIDADES:<br/>Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.</p> <p>• EXPLOTACIÓN:</p> <ul style="list-style-type: none"> <li>• Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo: <ul style="list-style-type: none"> <li>o Inyección de código</li> <li>o Inclusión de ficheros locales o remotos</li> <li>o Evasión de autenticación</li> <li>o Carencia de controles de autorización</li> <li>o Ejecución de comandos en el lado del servidor</li> <li>o Ataques tipo Cross Site Request Forgery</li> <li>o Control de errores</li> <li>o Gestión de sesiones</li> <li>o Fugas de información</li> <li>o Secuestros de sesión</li> <li>o Comprobación de las condiciones para realizar una denegación de servicio.</li> </ul> </li> </ul> <p>• POST EXPLOTACIÓN:<br/>En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adicionales con el objetivo de comprobar la criticidad de esta.</p> <p>No URL IP<br/>1.<br/><a href="https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz135.181.185.207">https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz135.181.185.207</a><br/>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> |                |
| Config | application-component |  | plataforma: cs |

| Name                    | Type                  | Description  | Properties                                   |
|-------------------------|-----------------------|--|--|
| Controlador admin       | application-component |  | <i>plataforma: cs</i>                        |
| Controlador frontal mvl | application-component |  | <i>plataforma: js</i>                        |
| Controlador frontal web | application-component | - Verificados los SSL, se recomienda adquirir SSL seguros, con entidades certificadoras.<br>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. | <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><br><i>brecha: 100</i> |
| Transacciones           | application-component |  | <i>plataforma: sql</i><br><i>brecha: 100</i> |
| Utilitario              | application-component |  | <i>plataforma: no-sql</i>                    |
| Vista móvil             | application-component |  | <i>plataforma: js</i>                        |

| 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<br/>"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<br/>"8C:48:BD:E2:F5:18:18:C3:85:96:68:44:2E:28:A0:68:08:2F:0A:BE"</p> | <i>plataforma:</i> 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<br/>"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<br/>"8C:48:BD:E2:F5:18:18:C3:85:96:68:44:2E:28:A0:68:08:2F:0A:BE"</p>  | <i>plataforma:</i> angular 11                       |
| API externas                     | application-service   |  |   |
| Application Service (NLB)        | application-service   |  | <i>plataforma:</i> angular 11<br><i>brecha:</i> 100 |
| Archivos Compartidos             | application-service   |  |   |
| CDN Contenidos                   | application-service   |  | <i>brecha:</i> 100                                  |
| Doku (gest. doc.)                | application-service   |  | <i>brecha:</i> 100                                  |
| Identidades                      | application-service   |  |   |
| Interfaz de datos 1              | application-service   |  |   |

| Name                        | Type                | Description   | Properties         |
|-----------------------------|---------------------|---|--------------------|
| Interfaz de datos 2         | application-service |   |                    |
| Interfaz de datos 3         | application-service |   |                    |
| cccc Proveedores contenidos | application-service |   | <i>brecha: 100</i> |
| Mensaje: JSON               | data-object         |   |                    |
| Infraestructura SUI         | grouping            | Soporte de infraestructura a los componentes del SUI Migración. Servidores y ambientes de cómputo para la ejecución del software base de los componentes misionales del SUI de PGN.   |                    |
| PGN SIU                     | grouping            | El objetivo principal de la arquitectura del SUI de la migración es la centralización de los conceptos misionales: concentrar los conceptos misionales en componentes aislados; dejar por fuera de estos componentes misionales todo lo distintos a la misionalidad de la PGN. Los objetivos secundarios de esta arquitectura SUI de la migración son flexibilidad y extensibilidad. Dichos objetivos son independientes. Es decir, estos pueden ser maximizados sin conflicto entre ellos. |                    |
| Servidor BDD App            | node                | Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz<br>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<br>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. |            |

## Lineabase.0.SIU aplicación. física

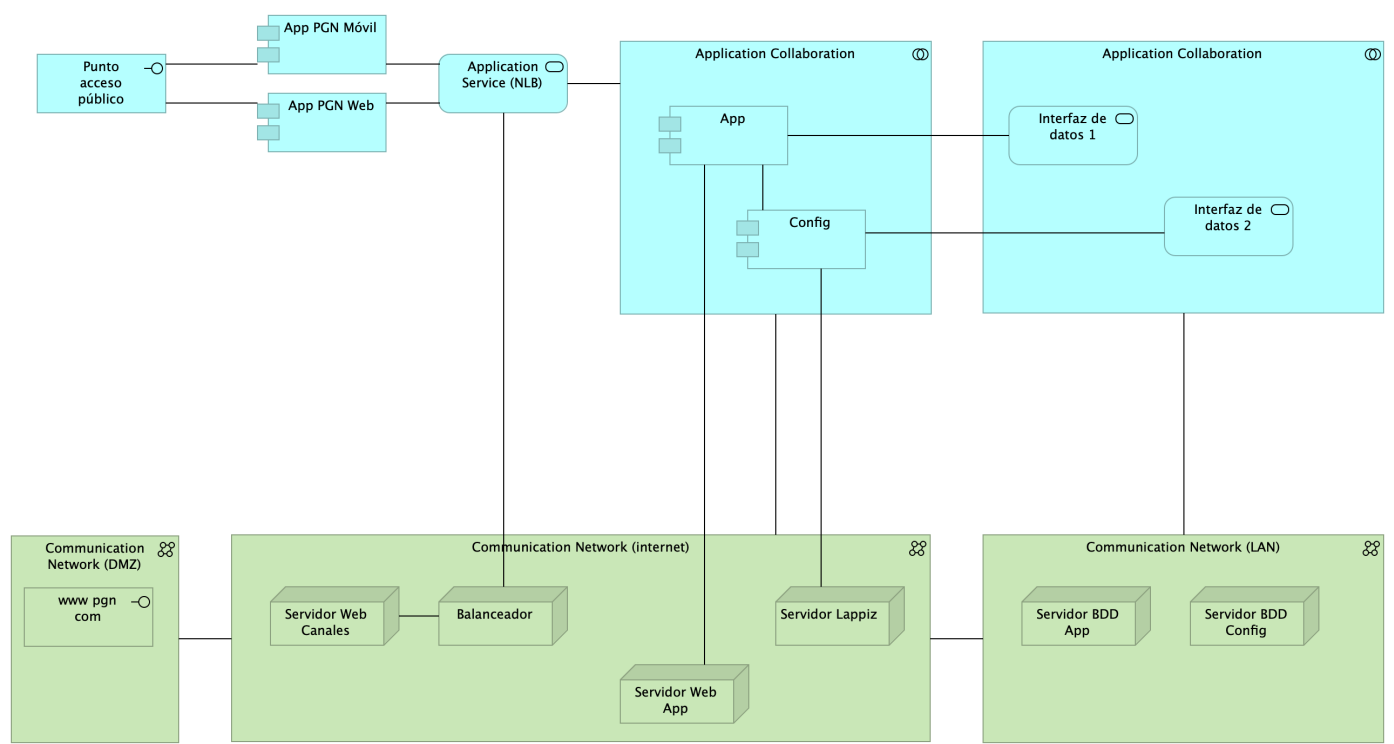


Imagen 2: Diagram: Lineabase.0.SIU aplicación. física

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     |  | <i>plataforma:</i> node Js<br><i>brecha:</i> 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. Protección de datos personales, Los sistemas de información que recogen, procesan y almacenan información de los derechos de las personas se deben almacenar de forma adecuada, la información que pueda ser vulnerada puede generar obliaciones legales y éticas con respecto a la perdida de informacion confidencial por parte de ciudadanos del pais. La informacion contenida en las bases de datos debe tener los mecanismos de cifrado que en otros apartados se han mencionado. La legislación que hay que tener como referencia, ley 1581 de 2012. Decreto 1377 de 2013 La metodologia empleada tendrá las siguientes fases:</p> <ul style="list-style-type: none"> <li>• FASE DE RECONOCIMIENTO:</li> </ul> <p>Se recolectará toda la información posible, usando diferentes técnicas</p> | <i>plantilla:</i> element-md-bold<br><i>brecha:</i> 100 |

| Name        | Type                  | Description  | Properties   |
|-------------|-----------------------|--|--|
|             |                       | <p>como:</p> <ul style="list-style-type: none"> <li>o Recopilación de dominios/IPs/puertos/servicios</li> <li>o Recopilación de metadatos</li> <li>o Uso de Google Dorks.</li> </ul> <p>• ANÁLISIS DE VULNERABILIDADES:<br/>Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.</p> <p>• EXPLOTACIÓN:</p> <ul style="list-style-type: none"> <li>• Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo: <ul style="list-style-type: none"> <li>o Inyección de código</li> <li>o Inclusión de ficheros locales o remotos</li> <li>o Evasión de autenticación</li> <li>o Carencia de controles de autorización</li> <li>o Ejecución de comandos en el lado del servidor</li> <li>o Ataques tipo Cross Site Request Forgery</li> <li>o Control de errores</li> <li>o Gestión de sesiones</li> <li>o Fugas de información</li> <li>o Secuestros de sesión</li> <li>o Comprobación de las condiciones para realizar una denegación de servicio.</li> </ul> </li> </ul> <p>• POST EXPLOTACIÓN:<br/>En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adicionales con el objetivo de comprobar la criticidad de esta.</p> <p>No URL IP<br/>1.<br/><a href="https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz">https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz</a><br/>135.181.185.207</p> |  |
| App PGN Web | application-component | A partir de los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la "Guía de desarrollo OWASP" y "OWAS Cheat Sheet, se realizaran pruebas de seguridad a   | <p><i>plataforma:</i> angular 11</p> <p><i>brecha:</i> 100</p> |

| Name | Type | Description  | Properties |
|------|------|--|------------|
|      |      | <p>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"> <li>• FASE DE RECONOCIMIENTO:<br/>Se recolectará toda la información posible, usando diferentes técnicas como: <ul style="list-style-type: none"> <li>o Recopilación de dominios/IPs/puertos/servicios</li> <li>o Recopilación de metadatos</li> <li>o Uso de Google Dorks.</li> </ul> </li> <li>• ANÁLISIS DE VULNERABILIDADES:<br/>Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.</li> <li>• EXPLOTACIÓN: <ul style="list-style-type: none"> <li>• Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo: <ul style="list-style-type: none"> <li>o Inyección de código</li> <li>o Inclusión de ficheros locales o remotos</li> <li>o Evasión de autenticación</li> <li>o Carencia de controles de autorización</li> <li>o Ejecución de comandos en el lado del servidor</li> <li>o Ataques tipo Cross Site Request Forgery</li> <li>o Control de errores</li> <li>o Gestión de sesiones</li> <li>o Fugas de información</li> <li>o Secuestros de sesión</li> <li>o Comprobación de las condiciones para realizar una denegación de servicio.</li> </ul> </li> </ul> </li> <li>• POST EXPLOTACIÓN:<br/>En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adicionales con el objetivo de comprobar la</li> </ul> |            |

| Name                                    | Type                  | Description   | Properties                                    |
|---|-----------------------|---|---|
|   |                       | <p>criticidad de esta.<br/>No URL IP<br/>1.<br/>https://runtime-test.lappiz.io<br/>/#/auth/login/PGN_Lappiz<br/>135.181.185.207<br/>El Login deberá evidenciar<br/>el control de errores, al<br/>momento de realizar la<br/>validación deberá mensaje<br/>de error para el caso que se<br/>autentique con<br/>credenciales erradas.</p> |   |
| <b>Config</b>                           | application-component |   | <i>plataforma: cs</i>                         |
| <b>Punto acceso público</b>             | application-interface | URL tipo C<br>HTTP  |   |
| <b>Application Service (NLB)</b>        | application-service   |   | <i>plataforma: angular 11<br/>brecha: 100</i> |
| <b>Interfaz de datos 1</b>              | application-service   |   |   |
| <b>Interfaz de datos 2</b>              | application-service   |   |   |
| <b>Communication Network (DMZ)</b>      | communication-network |   |   |
| <b>Communication Network (LAN)</b>      | communication-network |   |   |
| <b>Communication Network (internet)</b> | communication-network |   |   |
| <b>Balanceador</b>                      | node                  |   |   |
| <b>Servidor BDD App</b>                 | node                  | <p>Sistema Operativo Windows<br/>Server 2019 Standard o<br/>Datacenter x64. RAM 8 GB.<br/>CPU 64 Bits, 4 Cores &gt; 2<br/>Ghz<br/>Discos SO C: 126 GB,<br/>Backup E: 511 GB, SQL Data<br/>F: 510 GB, SQL Log G: 510<br/>GB, TempDB G: 63.6 GB.</p>  |   |
| <b>Servidor BDD Config</b>              | node                  | <p>Sistema Operativo Windows<br/>Server 2019 Standard o<br/>Datacenter x64. RAM 8 GB.<br/>CPU 64 Bits, 4 Cores &gt; 2<br/>Ghz<br/>Discos SO C: 80 GB, Backup<br/>E: 250 GB, SQL Data F: 250<br/>GB, SQL Log G: 250 GB,<br/>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. |            |
| www pgn com          | technology-interface |  |            |

## Seguridad.2. Lineabase.0.SIU Aplicación

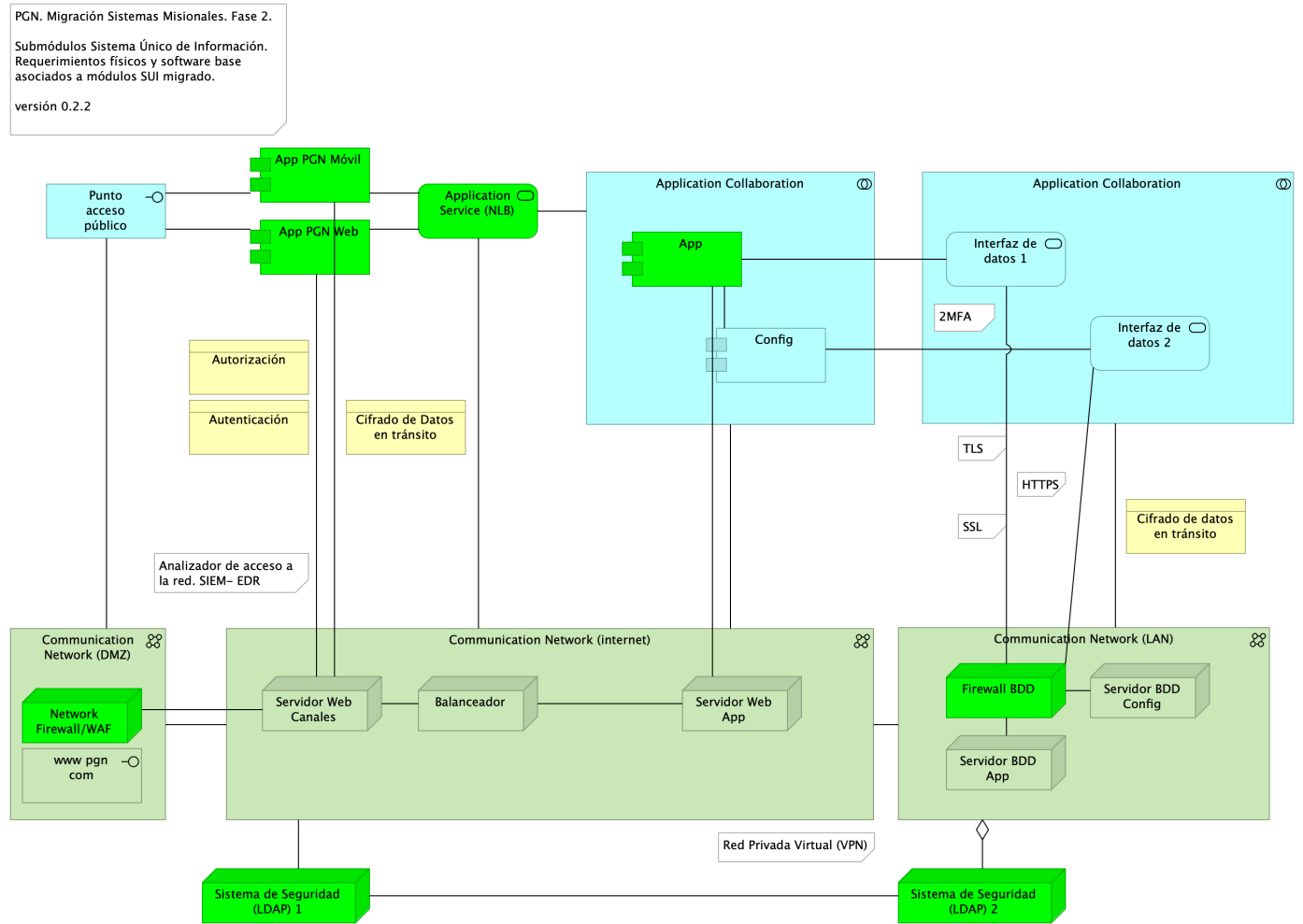


Imagen 3: Diagram: Seguridad.2. Lineabase.0.SIU Aplicación

## 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     |   | <i>plataforma:</i> node Js<br><i>brecha:</i> 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,</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"><li>• FASE DE RECONOCIMIENTO:</li></ul> <p>Se recolectará toda la información posible, usando diferentes técnicas como:</p> | <i>plantilla:</i> element-md-bold<br><i>brecha:</i> 100 |

| Name        | Type                  | Description  | Properties   |
|-------------|-----------------------|--|--|
|             |                       | <p>o Recopilación de dominios/IPs/puertos/servicios</p> <p>o Recopilación de metadatos</p> <p>o Uso de Google Dorks.</p> <p>• ANÁLISIS DE VULNERABILIDADES:</p> <p>Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.</p> <p>• EXPLOTACIÓN:</p> <p>• Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo:</p> <p>o Inyección de código</p> <p>o Inclusión de ficheros locales o remotos</p> <p>o Evasión de autenticación</p> <p>o Carencia de controles de autorización</p> <p>o Ejecución de comandos en el lado del servidor</p> <p>o Ataques tipo Cross Site Request Forgery</p> <p>o Control de errores</p> <p>o Gestión de sesiones</p> <p>o Fugas de información</p> <p>o Secuestros de sesión</p> <p>o Comprobación de las condiciones para realizar una denegación de servicio.</p> <p>• POST EXPLOTACIÓN:</p> <p>En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adicionales con el objetivo de comprobar la criticidad de esta.</p> <p>No URL IP</p> <p>1.</p> <p><a href="https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz">https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz</a></p> <p>135.181.185.207</p> |  |
| 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</p>   | <p><i>plataforma:</i> angular 11</p> <p><i>brecha:</i> 100</p> |

| Name | Type | Description   | Properties |
|------|------|---|------------|
|      |      | <p>vulnerabilidades, y pruebas de Ethical Hacking.</p> <p>Los resultados permitirán identificar los requisitos de seguridad que los sistemas de información o servicios web deberán cumplir.</p> <p>La metodología empleada tendrá las siguientes fases:</p> <ul style="list-style-type: none"> <li>• FASE DE RECONOCIMIENTO:<br/>Se recolectará toda la información posible, usando diferentes técnicas como: <ul style="list-style-type: none"> <li>o Recopilación de dominios/IPs/puertos/servicios</li> <li>o Recopilación de metadatos</li> <li>o Uso de Google Dorks.</li> </ul> </li> <li>• ANÁLISIS DE VULNERABILIDADES:<br/>Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.</li> <li>• EXPLOTACIÓN: <ul style="list-style-type: none"> <li>• Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo: <ul style="list-style-type: none"> <li>o Inyección de código</li> <li>o Inclusión de ficheros locales o remotos</li> <li>o Evasión de autenticación</li> <li>o Carencia de controles de autorización</li> <li>o Ejecución de comandos en el lado del servidor</li> <li>o Ataques tipo Cross Site Request Forgery</li> <li>o Control de errores</li> <li>o Gestión de sesiones</li> <li>o Fugas de información</li> <li>o Secuestros de sesión</li> <li>o Comprobación de las condiciones para realizar una denegación de servicio.</li> </ul> </li> </ul> </li> <li>• POST EXPLOTACIÓN:<br/>En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adicionales con el objetivo de comprobar la criticidad de esta.</li> </ul> |            |



| Name                             | Type                  | Description  | Properties  |
|----------------------------------|-----------------------|--|---|
|                                  |                       | <p>No URL IP</p> <p>1.<br/>https://runtime-test.lappiz.io/#/auth/login/PGN_Lappiz135.181.185.207</p> <p>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>  |   |
| <b>Config</b>                    | application-component |  | <i>plataforma: cs</i>                               |
| <b>Punto acceso público</b>      | application-interface | URL tipo C HTTP  |   |
| <b>Application Service (NLB)</b> | application-service   |  | <i>plataforma: angular 11</i><br><i>brecha: 100</i> |
| <b>Interfaz de datos 1</b>       | application-service   |  |   |
| <b>Interfaz de datos 2</b>       | application-service   |  |   |
| <b>Autenticación</b>             | 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)</p> |   |

| Name         | Type            | Description  | Properties |
|--------------|-----------------|--|------------|
|              |                 | <p>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</p>   |            |

| Name | Type | Description   | Properties |
|------|------|---|------------|
|      |      | <p>Interno y relatoría, entre otros.), y que se considera un mecanismo de protección, que ayuda a reaccionar ante cualquier operación no autorizada. El control de acceso basado en roles (RBAC), enfoca la idea de que a los funcionarios se les otorgue los permisos de acceso a los recursos, basados en los roles y/o perfiles que este posee. Este control posee dos características fundamentales: i) los accesos son controlados por medio de los roles y/o perfiles asignados, quiere decir, a los servidores públicos, contratistas, terceros y otros colaboradores autorizados para interactuar con los sistemas de información se le asignan los roles y el encargado/responsable definirá los permisos, que a su vez están relacionados con los roles, ii) Los roles pueden ser definidos a nivel jerárquico, es decir que un rol podrá ser miembro de otro rol. Un proceso de autorización basado en roles, identifica tres factores importantes, i) Todos los servidores públicos, contratistas, terceros y otros Colaboradores, deben tener un rol asignado, si no es asignado no podrá realizar ninguna acción relacionada con el acceso, ii) un usuario podrá hacer uso de los permisos asociados a los roles asignados, el cual deberá realizar el inicio de sesión el usuario asignado del Directorio activo (DA), iii) los servidores públicos, contratistas, terceros y otros, solo podrán realizar acciones para las cuales han sido autorizados por medio de la activación de sus roles y/o perfiles. EL control definido para los accesos basados en roles RBAC, permitirá que solo</p> |            |

| Name | Type | Description   | Properties |
|------|------|---|------------|
|      |      | <p>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. 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</p> |            |

| Name | Type | Description  | Properties |
|------|------|--|------------|
|      |      | <p>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</p> |            |

| Name | Type | Description  | Properties |
|------|------|--|------------|
|      |      | <p>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<br/>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:<br/>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<br/>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<br/>Este ítem establece el proceso adecuado para el</p> |            |

| Name | Type | Description   | Properties |
|------|------|---|------------|
|      |      | <p>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 niveles de accesos requeridos, (Consultar, Modificar, Eliminar) (CRUD) y iv) Tipos de usuarios, roles que pueden ser asignados</p> |            |

| Name | Type | Description   | Properties |
|------|------|---|------------|
|      |      | <p>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 Criptográficas.</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 PGN.</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> |            |

| Name                                | Type                  | Description  | Properties |
|-------------------------------------|-----------------------|--|------------|
| <b>Cifrado de datos en tránsito</b> | business-object       | <p>Proteger la información propia de la PGN utilizando mecanismos de cifrado que permita garantizar los pilares de Seguridad de la Información</p> <p>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> |            |
| <b>Communication Network (DMZ)</b>  | communication-network |  |            |

| Name                                    | Type                  | Description  | Properties         |
|---|-----------------------|--|--------------------|
| <b>Communication Network (LAN)</b>      | communication-network |  |                    |
| <b>Communication Network (internet)</b> | communication-network |  |                    |
| <b>Balanceador</b>                      | node                  |  |                    |
| <b>Firewall BDD</b>                     | node                  |  | <i>brecha: 100</i> |
| <b>Network Firewall/WAF</b>             | node                  |  | <i>brecha: 100</i> |
| <b>Servidor BDD App</b>                 | node                  | Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz<br>Discos SO C: 126 GB, Backup E: 511 GB, SQL Data F: 510 GB, SQL Log G: 510 GB, TempDB G: 63.6 GB.  |                    |
| <b>Servidor BDD Config</b>              | node                  | Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz<br>Discos SO C: 80 GB, Backup E: 250 GB, SQL Data F: 250 GB, SQL Log G: 250 GB, TempDB G: 30 GB.     |                    |
| <b>Servidor Web App</b>                 | 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. |                    |
| <b>Servidor Web Canales</b>             | 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. |                    |

| Name                                 | Type                 | Description  | Properties         |
|--------------------------------------|----------------------|--|--------------------|
| <b>Sistema de Seguridad (LDAP) 1</b> | node                 | Sistema de Seguridad (LDAP) 1. Control de acceso internet,<br>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> |
| <b>Sistema de Seguridad (LDAP) 2</b> | node                 | Sistema de Seguridad (LDAP) 2. Control de acceso internet,<br>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> |
| <b>www pgn com</b>                   | technology-interface |  |                    |

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

## Requerimientos de Administración

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

8. Las soluciones deben permitir la definición de varios tipos de usuario.
9. Las soluciones deben permitir la parametrización de los consecutivos que maneja la entidad para los diferentes documentos generados por las soluciones.
10. Debe permitir parametrizar la vinculación del consecutivo a un documento en forma manual o automática.
11. Las soluciones deben permitir que se configure la autenticación de forma interna integrándose con LDAP el acceso de los usuarios y actores de las diferentes dependencias de la entidad que interactúen con los demás sistemas.

## Requerimientos de Seguridad

---

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

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

# 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/>