Documento de Arquitectura Migración Funcional PGN SIU

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

Versión del producto 1.d98c640 de 09 Nov 2023
Presentado a
Procuraduría General de la Nación (PGN)
Fecha
09 Nov 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@d98c640 del November 9, 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.d98c640	2023-11-09. tema–tablas
1.aecc652	2023-11-09. crrcn–txt-10
1.1bbd2b1	2023-11-08. corrcn–sgrdd5
1.1bbb460	2023-11-08. corrcn–sgrdd4
1.8e9dee0	2023-11-08. corrcn–sgrdd3
1.00eb497	2023-11-08. corrcn–sgrdd
1.2c588a4	2023-11-08. cnsdrcns–sgrdd
1.c717651	2023-11-08. pgndoc–crrcntxt
1.6e4e675	2023-11-08. pgndoc
1.fa97e14	2023-11-08. arqdoc2
Vínculos	N003a Vista Segmento PGN SIU

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 Particulares de Arquitectura (no funcional)

Consistencia SUI (lógica)

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

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

Mantenibilidad SUI

Tabla 2: Requisito no. 2, Mantenibilidad SUI.

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

Extensibilidad SUI

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

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

Arquitectura de Software

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

Diagrama de Arquitectura de la Solución Propuesta: vista de integración

Migracion.1a.b.SIU Contexto Módulos

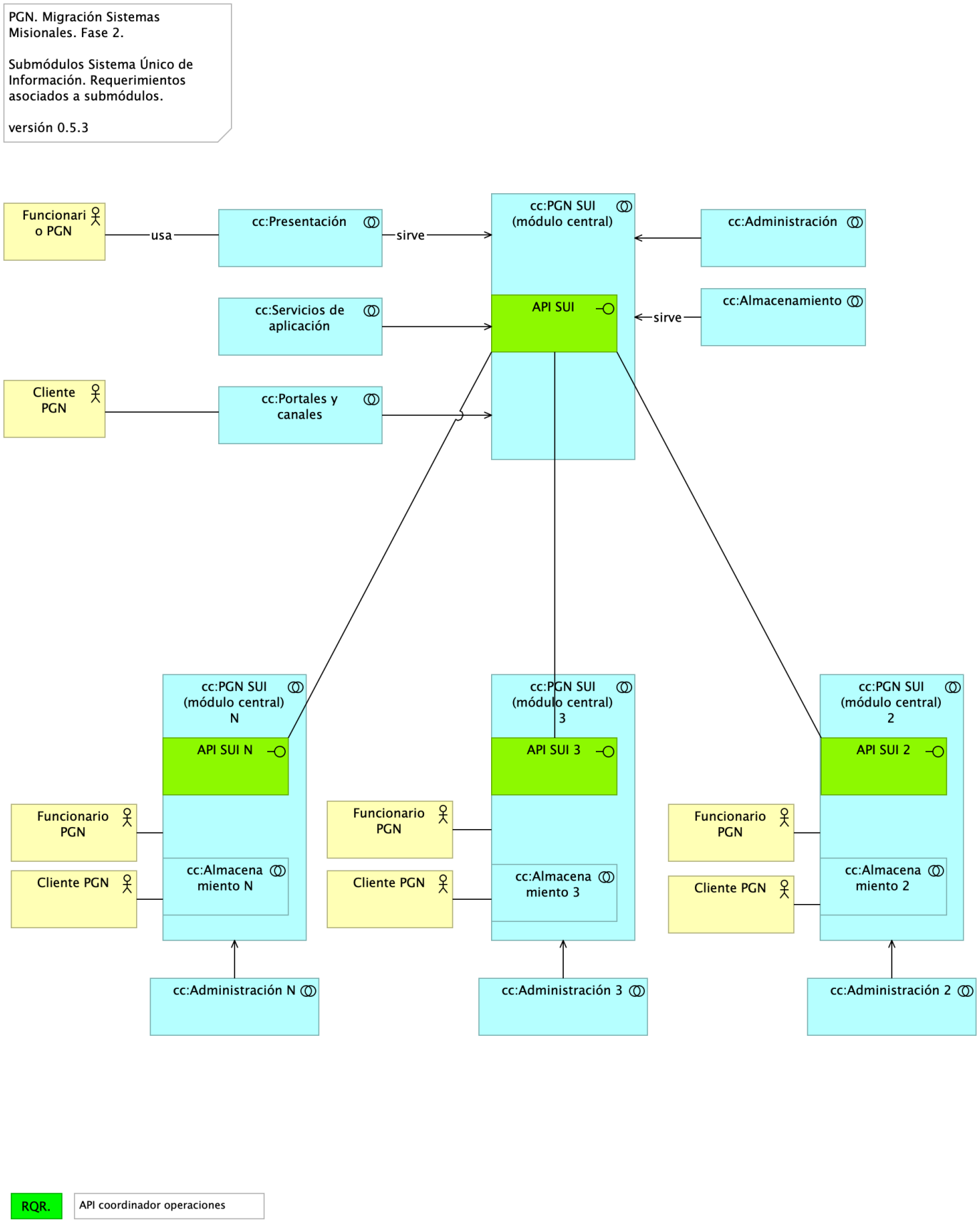


Imagen 1: Vista. Migracion.1a.b.SIU Contexto Módulos

La vista presenta en contexto a los módulos SUI migrados y el estilo de comunicación vía API sincrónica/asincrónica (en verde en la imagen).

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

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

La coordinación de transacciones es realizada por la colaboración de las otras API individuales de cada módulo. Por ejemplo, si una relatoría nueva requiere alguna validación de Hominis, el módulo coordinador (c) inicia la transacción hacia Homini, y este, el módulo proveedor (p) responde con el resultado de la validación. Esta módulo coordinador misma operación se repite cuando la transacción involucra a más módulos proveedores (p).

Catálogo de Elementos

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

Nombre	Tipo	Descripción	Prop.
Funcionario PGN	business-actor		
Funcionario PGN	business-actor		
Funcionario PGN	business-actor		
Funcionario PGN	business-actor		

Migracion.1a.a.SIU Contexto Módulo

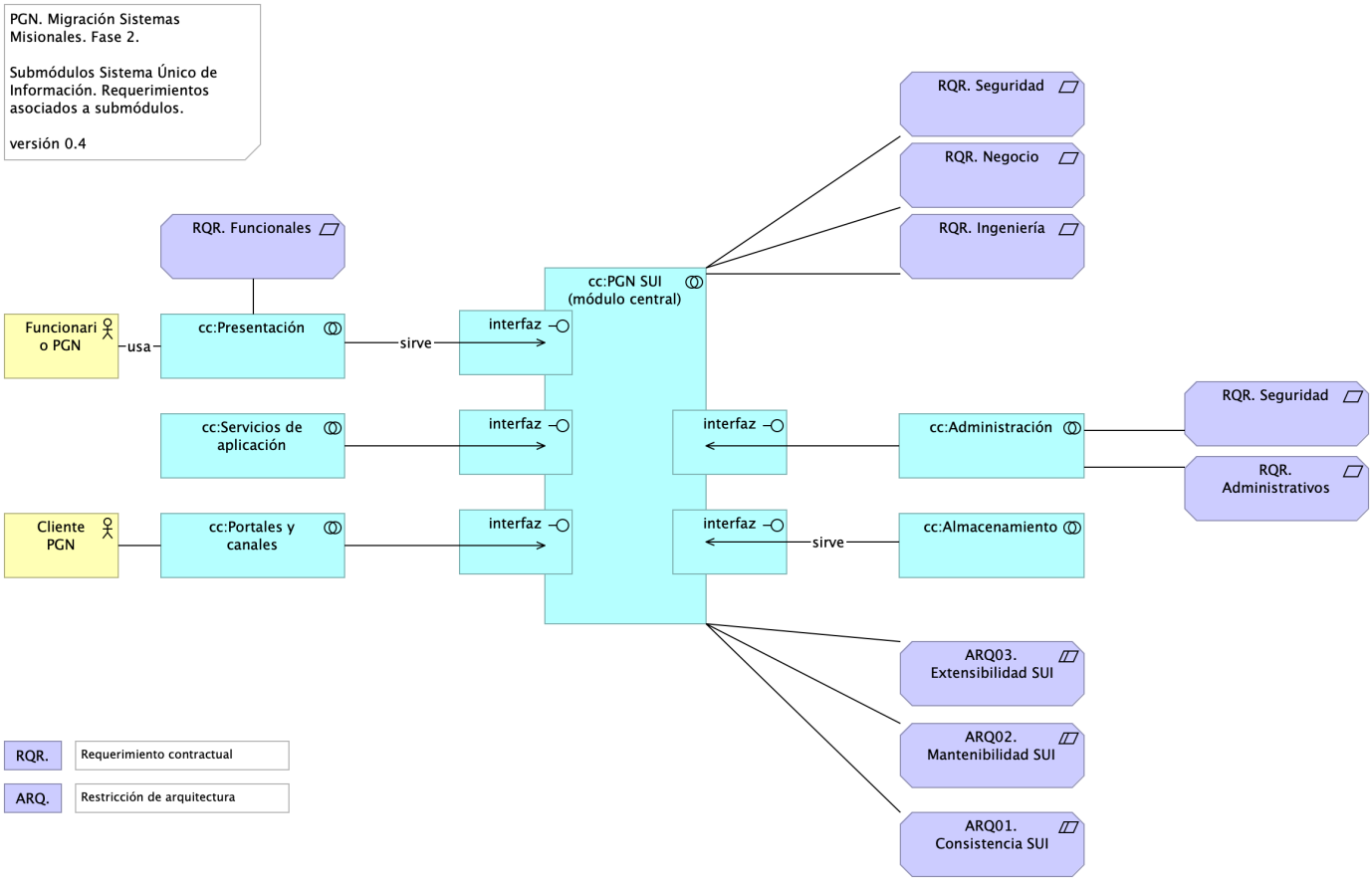


Imagen 2: Vista. Migracion.1a.a.SIU Contexto Módulo

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

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

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

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

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

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

Requerimientos Asociados a los Submódulos

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

Catálogo de Elementos

Nombre	Tipo	Descripción	Prop.
cc:Administración	application-collaboration		
cc:Almacenamiento	application-collaboration	Espacio de almacenamiento operativo y transaccional de un módulo central del SUI migrado.	
cc:PGN SUI (módulo central)	application-collaboration	Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular de la PGN.	
cc:Portales y canales	application-collaboration	Submódulo de portales internos de la PGN a donde llega el SUI. Interfaz web que usa al SUI para llegar a direcciones y subdirecciones de la PGN. La plataforma principal de portales en este contexto es SharePoint de Microsoft.	
cc:Presentación	application-collaboration	Submódulo de presentación del SUI. interfaz gráfica, interfaz web visible a los usuarios clientes y funcionarios de la PGN.	
cc:Servicios de aplicación	application-collaboration	Submódulo de servicios utilitarios que sirven al SUI. Servicios variados que cumplen roles facilitadores de las actividades misionales del SUI. Ejemplos de estos servicios son los de gestión documental, implementado por Doku en el contexto de PGN.	
interfaz	application-interface		
interfaz	application-interface		
interfaz	application-interface		
interfaz	application-interface		
interfaz	application-interface		
Cliente PGN	business-actor		
Funcionario PGN	business-actor		
ARQ01. Consistencia SUI	constraint	Unifica las entidades de negocio PGN, entre las que se incluyen a conciliaciones, publicaciones de relatoría, resoluciones, en artefactos reutilizables. Distinto de que estas entidades (y su lógica de negocio) estén dispersos entre los sistemas del SUI, estarán concentradas en un único artefacto correspondiente. Calidad sistémica: la consistencia persigue que el resultado de la lógica de negocio sea la misma entre los módulos del SUI migrado. Esto redunda a mantenibilidad y gestión: tiende a tener un solo punto de cambio y dificulta la transferencia de dependencias implícitas a otros procesos.	
ARQ02. Mantenibilidad SUI	constraint	Evitar las dependencia transitivas de los módulos misionales del SUI a componentes y sistemas de terceros o submódulos no misionales. Calidad sistémica: la mantenibilidad por control de dependencias que optimiza el diseño Migración SUI está dada por el control de cambios no programados sobre los componentes misionales del SUI (corrupción de componentes). Ver Patrón de Diseño Migración SUI, más adelante en el documento.	
ARQ03. Extensibilidad SUI	constraint	Concentración de los componentes de negocio, misionales, del SUI protegidos de cambios provenientes de otros sistemas. Ver Patrón de Diseño Migración SUI, más adelante en el documento. Calidad sistémica: la extensibilidad que optimiza el diseño Migración SUI está dada por el intercambio de submódulos no misionales, como el gestor documental, sin afectación de los componentes misionales que este diseño protege.	
RQR. Administrativos	requirement		
RQR. Funcionales	requirement		
RQR. Ingeniería	requirement		
RQR. Negocio	requirement		
RQR. Seguridad	requirement	Requerimientos de seguridad, SUI, Migración, en aspectos de comunicación, autenticación, autorización y (manejo de) sesiones.	

Nombre	Tipo	Descripción	Prop.
RQR. Seguridad	requirement	Requerimientos de seguridad, SUI, Migración, en aspectos de comunicación, autenticación, autorización y (manejo de) sesiones.	

Diagrama de Arquitectura de la solución propuesta: vista física

Lineabase.0.SIU Aplicación. Física

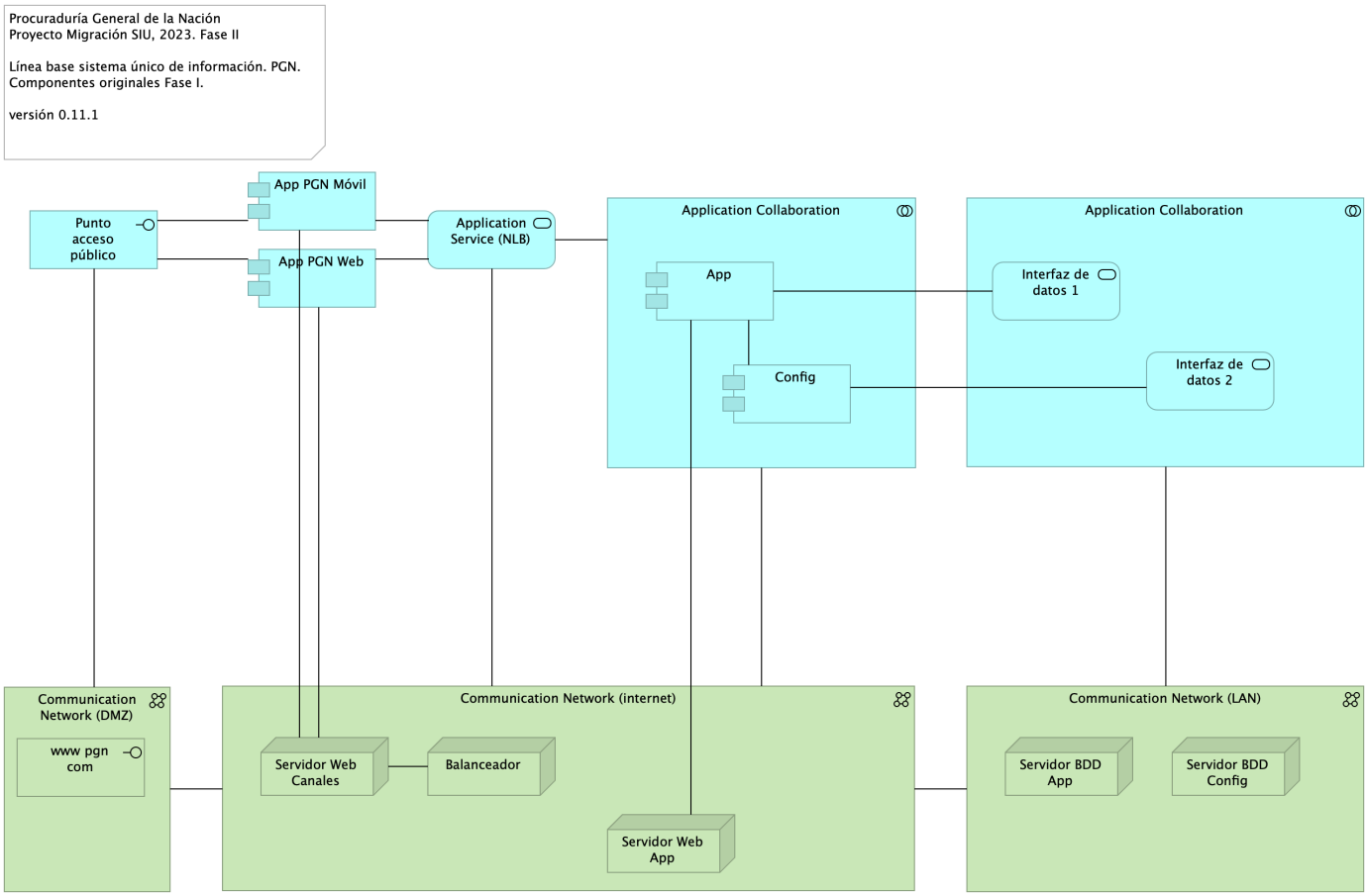


Imagen 3: Vista. Lineabase.0.SIU Aplicación. Física

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

Nombre	Tipo	Descripción	Prop.
Application Collaboration	application-collaboration		
Application Collaboration	application-collaboration		
App	application-component		*plataforma:* node Js *brecha:* 100
App PGN Móvil	application-component		*plantilla:* element-md-bold *brecha:* 100
App PGN Web	application-component		*plataforma:* angular 11 *brecha:* 100
Config	application-component		*plataforma:* cs
Punto acceso público	application-interface	URL tipo C HTTP	
Application Service (NLB)	application-service		*plataforma:* angular 11 *brecha:* 100
Interfaz de datos 1	application-service		

Nombre	Tipo	Descripción	Prop.
Interfaz de datos 2	application-service		
Communication Network (DMZ)	communication-network		
Communication Network (LAN)	communication-network		
Communication Network (internet)	communication-network		
Balanceador	node		
Servidor BDD App	node	Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz. Discos SO C: 126 GB, Backup E: 511 GB, SQL Data F: 510 GB, SQL Log G: 510 GB, TempDB G: 63.6 GB.	
Servidor BDD Config	node	Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz. Discos SO C: 80 GB, Backup E: 250 GB, SQL Data F: 250 GB, SQL Log G: 250 GB, TempDB G: 30 GB.	
Servidor Web App	node	Windows Server 2019 Standard o Datacenter x64. Nombre físico. IP LAN. IP Pública. Windows Server 2019 Standard or Datacenter x64. RAM 8 GB. CPU 64 Bits. 4 Cores de 2 Ghz. Discos SO C: 126 GB. SO D: 16 GB.	
Servidor Web Canales	node	Windows Server 2019 Standard o Datacenter x64. Nombre físico. IP LAN. IP Pública. Windows Server 2019 Standard or Datacenter x64. RAM 8 GB. CPU 64 Bits. 4 Cores de 2 Ghz. Discos SO C: 126 GB. SO D: 16 GB.	
www pgn com	technology-interface		

Diagrama de Arquitectura de la Solución Propuesta: motivadores del negocio

Migracion.1a.a.SIU Contexto Módulo

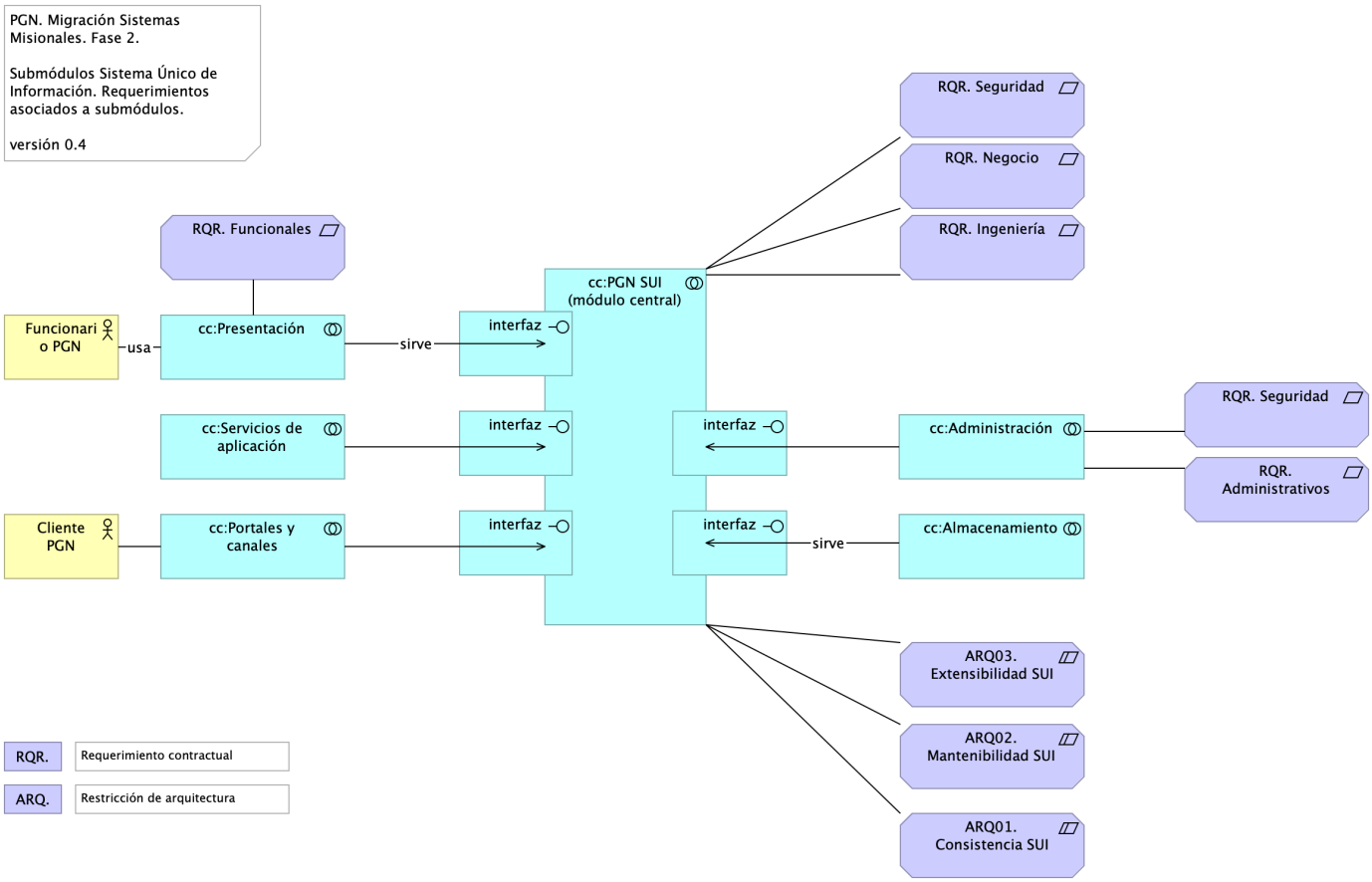


Imagen 4: Vista. Migracion.1a.a.SIU Contexto Módulo

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

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

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

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

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

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

Requerimientos Asociados a los Submódulos

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

Catálogo de Elementos

Nombre	Tipo	Descripción	Prop.
cc:Administración	application-collaboration		

Nombre	Tipo	Descripción	Prop.
cc:Almacenamiento	application-collaboration	Espacio de almacenamiento operativo y transaccional de un módulo central del SUI migrado.	
cc:PGN SUI (módulo central)	application-collaboration	Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular de la PGN.	
cc:Portales y canales	application-collaboration	Submódulo de portales internos de la PGN a donde llega el SUI. Interfaz web que usa al SUI para llegar a direcciones y subdirecciones de la PGN. La plataforma principal de portales en este contexto es SharePoint de Microsoft.	
cc:Presentación	application-collaboration	Submódulo de presentación del SUI. interfaz gráfica, interfaz web visible a los usuarios clientes y funcionarios de la PGN.	
cc:Servicios de aplicación	application-collaboration	Submódulo de servicios utilitarios que sirven al SUI. Servicios variados que cumplen roles facilitadores de las actividades misionales del SUI. Ejemplos de estos servicios son los de gestión documental, implementado por Doku en el contexto de PGN.	
interfaz	application-interface		
interfaz	application-interface		
interfaz	application-interface		
interfaz	application-interface		
interfaz	application-interface		
Cliente PGN	business-actor		
Funcionario PGN	business-actor		
ARQ01. Consistencia SUI	constraint	Unifica las entidades de negocio PGN, entre las que se incluyen a conciliaciones, publicaciones de relatoría, resoluciones, en artefactos reutilizables. Distinto de que estas entidades (y su lógica de negocio) estén dispersos entre los sistemas del SUI, estarán concentradas en un único artefacto correspondiente. Calidad sistémica: la consistencia persigue que el resultado de la lógica de negocio sea la misma entre los módulos del SUI migrado. Esto redunda a mantenibilidad y gestión: tiende a tener un solo punto de cambio y dificulta la transferencia de dependencias implícitas a otros procesos.	
ARQ02. Mantenibilidad SUI	constraint	Evitar las dependencia transitivas de los módulos misionales del SUI a componentes y sistemas de terceros o submódulos no misionales. Calidad sistémica: la mantenibilidad por control de dependencias que optimiza el diseño Migración SUI está dada por el control de cambios no programados sobre los componentes misionales del SUI (corrupción de componentes). Ver Patrón de Diseño Migración SUI, más adelante en el documento.	
ARQ03. Extensibilidad SUI	constraint	Concentración de los componentes de negocio, misionales, del SUI protegidos de cambios provenientes de otros sistemas. Ver Patrón de Diseño Migración SUI, más adelante en el documento. Calidad sistémica: la extensibilidad que optimiza el diseño Migración SUI está dada por el intercambio de submódulos no misionales, como el gestor documental, sin afectación de los componentes misionales que este diseño protege.	
RQR. Administrativos	requirement		
RQR. Funcionales	requirement		
RQR. Ingeniería	requirement		
RQR. Negocio	requirement		
RQR. Seguridad	requirement	Requerimientos de seguridad, SUI, Migración, en aspectos de comunicación, autenticación, autorización y (manejo de) sesiones.	
RQR. Seguridad	requirement	Requerimientos de seguridad, SUI, Migración, en aspectos de comunicación, autenticación, autorización y (manejo de) sesiones.	

Riesgos.1. Migración funcional

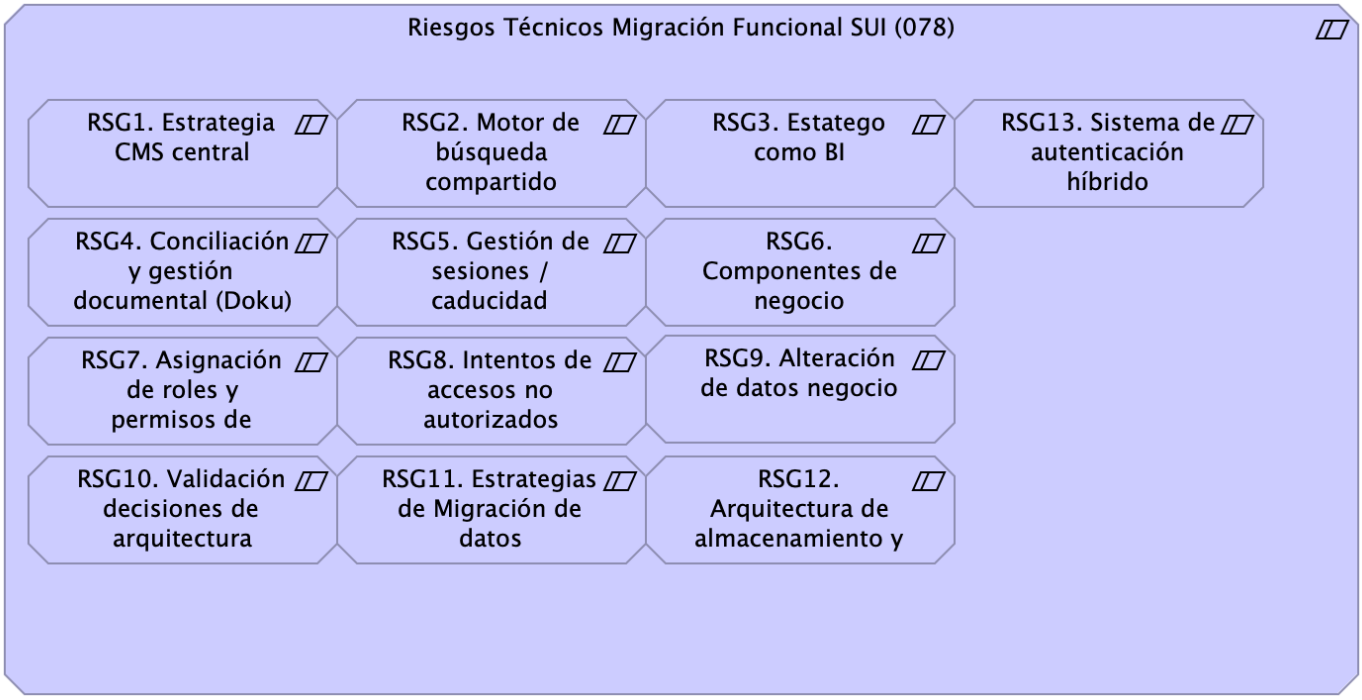


Imagen 5: Vista. Riesgos.1. Migración funcional

Riesgos de la migración funcional:

- RSG1. Estrategia CMS central
- RSG2. Motor de búsqueda
- RSG3. Estratego como BI
- RSG4. Conciliación y Doku
- RSG5. Gestión de sesiones / caducidad
- RSG6. Componentes de negocio
- RSG7. Asignación de roles y permisos de Acceso
- RSG8. Intentos de accesos no autorizados
- RSG9. Alteración de datos negocio
- RSG10. Validación decisiones de arquitectura
- RSG11. Estrategias de Migración de datos
- RSG12. Arquitectura de almancenamiento y distribución de datos SIU
- RSG13. Sistema de autenticación híbrido

Acciones de Mitigación

1. Informar a la PGN de las implicaciones junto con alternativas para la implementación de la acción de aprovechamiento: diseño del SCM central (SharePoint). La PGN debe decidir si o no a la acción propuesta.

2. Informar a la PGN de las implicaciones junto con alternativas para la implementación de la acción de aprovechamiento: diseño del motor de búsqueda compartido (SharePoint). La PGN debe decidir si o no a la acción propuesta.

3. Informar a la PGN de las implicaciones junto con alternativas para la implementación de la acción de manejo del riesgo: diseño de solución de inteligencia de negocio (Power BI). La PGN debe decidir si o no a la acción propuesta.

4. Informar a la PGN de las implicaciones junto con alternativas para la implementación de la acción de manejo del riesgo: ubicar la lógica, los flujos, y los datos misionales dentro del SIU. La PGN debe decidir si o no a la acción propuesta.

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

Catálogo de Elementos

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

Nombre	Tipo	Descripción	Prop.
RSG10. Validación decisiones de arquitectura	constraint	Discutir la arquitectura de referencia de SUI Migración PGN. La arquitectura de referencia SUI informa de todas las fortalezas y consideraciones estructurales y de sistema, como extensibilidad, rendimiento y seguridad, que regirán a todos los módulos del SUI migrado.	
RSG11. Estrategias de Migración de datos	constraint	Discutir el alcance y los recursos para la correcta migración de datos incluídas en contrato 078, Migración Funcional SIU en atención al numeral 5.6 del anexo técnico del proyecto.	5.6 MIGRACIÓN DE DATOS
RSG12. Arquitectura de almacenamiento y distribución de datos SIU	constraint	Definir la opción de organización y distribución de los almacenes de datos del SIU. opc1. Dispositivo físico/virtual (nodo, servidor, y esquema de base de datos) único, central, a todos los módulos del SIU. opc2. Dispositivos virtuales autónomos por dominio de negocio: rlatoría, inventario, información estratégica, intercomunicados.	
RSG13. Sistema de autenticación híbrido	constraint	Definir la estrategia de autenticación del SIU migrado (aplicable a todos los módulos del SIU migrado). opc1. Híbrida: integrado, directorio empresarial (LDAP), y servicios de autenticación de confianza: Office 365 de PGN. opc2. Servicio de autenticación de confianza: Office 365 de PGN.	
RSG2. Motor de búsqueda compartido	constraint	Establecer desde el principio el motor de búsqueda de conteidos compartido para los módulos del SUI migrados.	
RSG3. Estatego como BI	constraint	Definir la arquitectura de Estratego migrado: puede ser una solución de BI simple, o puede ser una aplicación web tradicional.	
RSG4. Conciliación y gestión documental (Doku)	constraint	Definir la ubicación de los componentes misionales de Conciliación Administrativa (SIU). Debe estar fuera de Doku.	
RSG5. Gestión de sesiones / caducidad	constraint	Establecer desde el principio el motor de búsqueda de conteidos compartido para los módulos del SUI migrados.	
RSG6. Componentes de negocio	constraint	Incluir el esfuerzo de creación de componentes estrcturales y comunes a los módulos del SUI migrado requeridos por la arquitectura de referencia SUI. Algunos componentes requeridos son: * Administración de autorizaciones (integrado con el directorio PGN) * Motor de flujos de trabajo para diseño y organización del trabajo (Conciliación) * Componente de ruteo de documentos (Relatoría)	
RSG7. Asignación de roles y permisos de Acceso	constraint	RSG7. Asignación de roles y permisos de Acceso Los riesgos de autenticación como el Single Sign On (SSO), permite que si las credenciales de usuario se ven comprometidas, pueden dar permiso a un atacante acceder a todos o la mayoría de recursos y aplicaciones en la red. Se ha propuesto controlar los accesos a partir de la documentación que identifica la metodología de clasificación y gestión de usuarios roles y procesos de autenticación, a partir del control de acceso basado en roles RBAC (Identidades y autenticación), que permite tener una reacción más oportuna para controlar los accesos a diferentes módulos de los diferentes sistemas de Información. Los inicios de sesión de los usuarios asociados a cuenta de dominio de Active Directory deben tener en cuenta la asignación de roles de ingreso al servidor o roles de ingreso al motor de bases de datos. Las cuentas de usuario no deben ser creadas de administrador local (administrador), es una puerta de entrada para los ataques de fuerza bruta.	

Nombre	Tipo	Descripción	Prop.
RSG8. Intentos de accesos no autorizados	constraint	RSG8. Intentos de accesos no autorizados Los intentos no autorizados son una de las técnicas más comunes utilizadas en la actualidad, los diferentes tipos de amenazas de intrusiones SQL Injections, Denegaciones de Servicios, riesgos de Ransomware, Ingeniería social, malware y otras amenazas, permite que se proponga implementación de soluciones de Seguridad perimetral a partir de la implementación de WAF para controlar las peticiones externas y evaluación de vulnerabilidades y escaneo para conocer puertos abiertos y establecer medidas.	
RSG9. Alteración de datos negocio	constraint	RSG9. Alteración de datos almacenados en Base de Datos. Se deberán asignar usuarios para la conexión de cada base de datos. Se debe proporcionar seguridad a nivel de filas y columnas (ofuscamiento) para proteger los datos confidenciales en el nivel de columnas y filas RLS ((seguridad de nivel de fila). Algunos de los métodos y características que se deben tener en cuenta a implementar es a partir del Alway encrypted, para cifrar los datos que se encuentran almacenados.	
Riesgos Técnicos Migración Funcional SUI (078)	constraint	Conjunto de riesgos técnicos y arquitectura. Proyecto Migración SUI 2023, PGN.	

Riesgos.2. Modelo Riesgo RSG10

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

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

versión 0.5

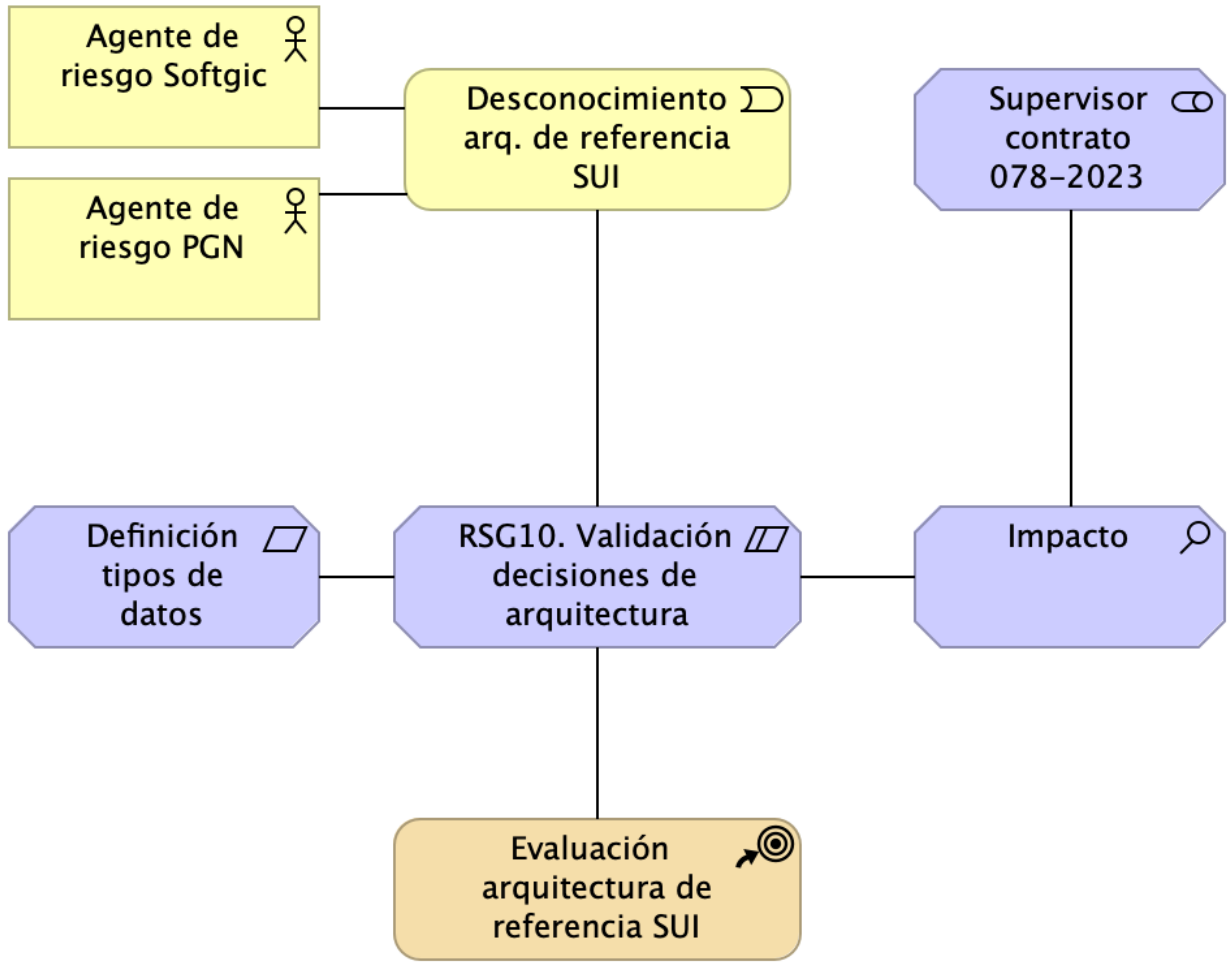


Imagen 6: Vista. Riesgos.2. Modelo Riesgo RSG10

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

Valoración del Riesgo

Tabla 4: Valoración del riesgo RSG10. Validación decisiones de arquitectura. Migración SUI.

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

Catálogo de Elementos

Nombre	**Tipo**	**Descripción**	**Prop.**
Impacto	assessment		

Nombre	Tipo	Descripción	Prop.
Agente de riesgo PGN	business-actor	Arquitecto PGN	
Agente de riesgo Softgic	business-actor	Arquitecto Softgic	
Desconocimiento arq. de referencia SUI	business-event		
RSG10. Validación decisiones de arquitectura	constraint	Discutir la arquitectura de referencia de SUI Migración PGN. La arquitectura de referencia SUI informa de todas las fortalezas y consideraciones estructurales y de sistema, como extensibilidad, rendimiento y seguridad, que regirán a todos los módulos del SUI migrado.	
Evaluación arquitectura de referencia SUI	course-of-action	La frecuencia del proceso de evaluación de la arquitectura es eventual, mínimo una vez cada dos semanas.	
Definición tipos de datos módulos SUI	requirement		
Supervisor contrato 078-2023	stakeholder		

Riesgos.3. Modelo Riesgo RSG11

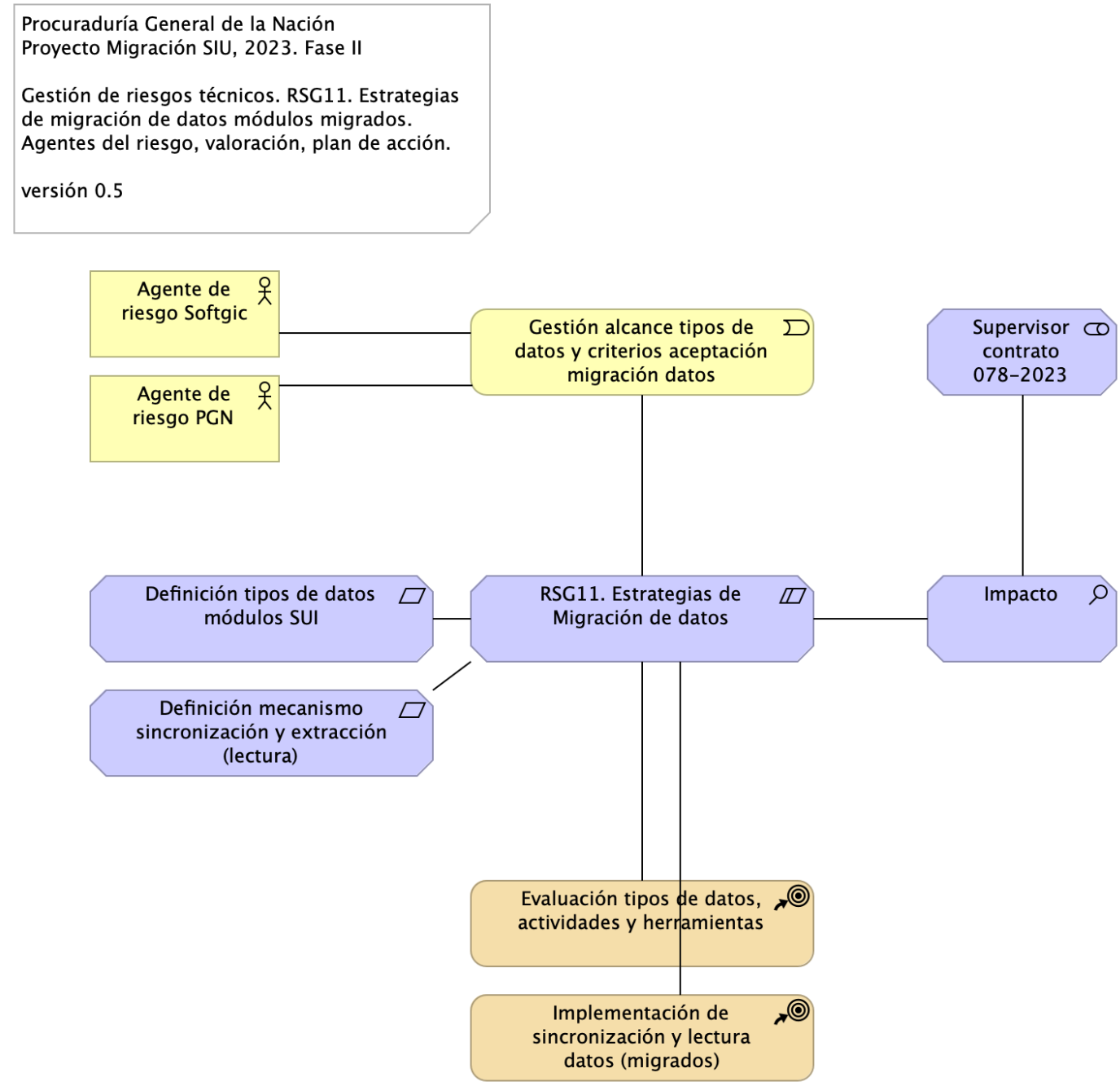


Imagen 7: Vista. Riesgos.3. Modelo Riesgo RSG11

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

Valoración del Riesgo

Tabla 5: Valoración del riesgo RSG10. Validación decisiones de arquitectura. Migración SUI.

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

Catálogo de Elementos

Nombre	**Tipo**	**Descripción**	**Prop.**
Impacto	assessment	Sobretrabajo del proyecto 078, esfuerzo y presupuesto.	
Agente de riesgo PGN	business-actor	Arquitecto PGN	
Agente de riesgo Softgic	business-actor	Arquitecto Softgic	
Gestión alcance tipos de datos y criterios aceptación migración datos	business-event		
RSG11. Estrategias de Migración de datos	constraint	Discutir el alcance y los recursos para la correcta migración de datos incluídas en contrato 078, Migración Funcional SIU en atención al numeral 5.6 del anexo técnico del proyecto.	5.6 MIGRACIÓN DE DATOS
Evaluación tipos de datos, actividades y herramientas	course-of-action	La frecuencia del proceso de evaluación de la arquitectura es eventual, mínimo una vez cada dos semanas.	
Implementación de sincronización y lectura datos (migrados)	course-of-action	La frecuencia del proceso de evaluación de la arquitectura es eventual, mínimo una vez cada dos semanas.	
Definición mecanismo sincronización y extracción (lectura)	requirement		
Definición tipos de datos módulos SUI	requirement		
Supervisor contrato 078-2023	stakeholder		

Diagrama de Arquitectura de la Solución Propuesta: interoperabilidad

Migracion.1c.SIU Módulos Colaboración

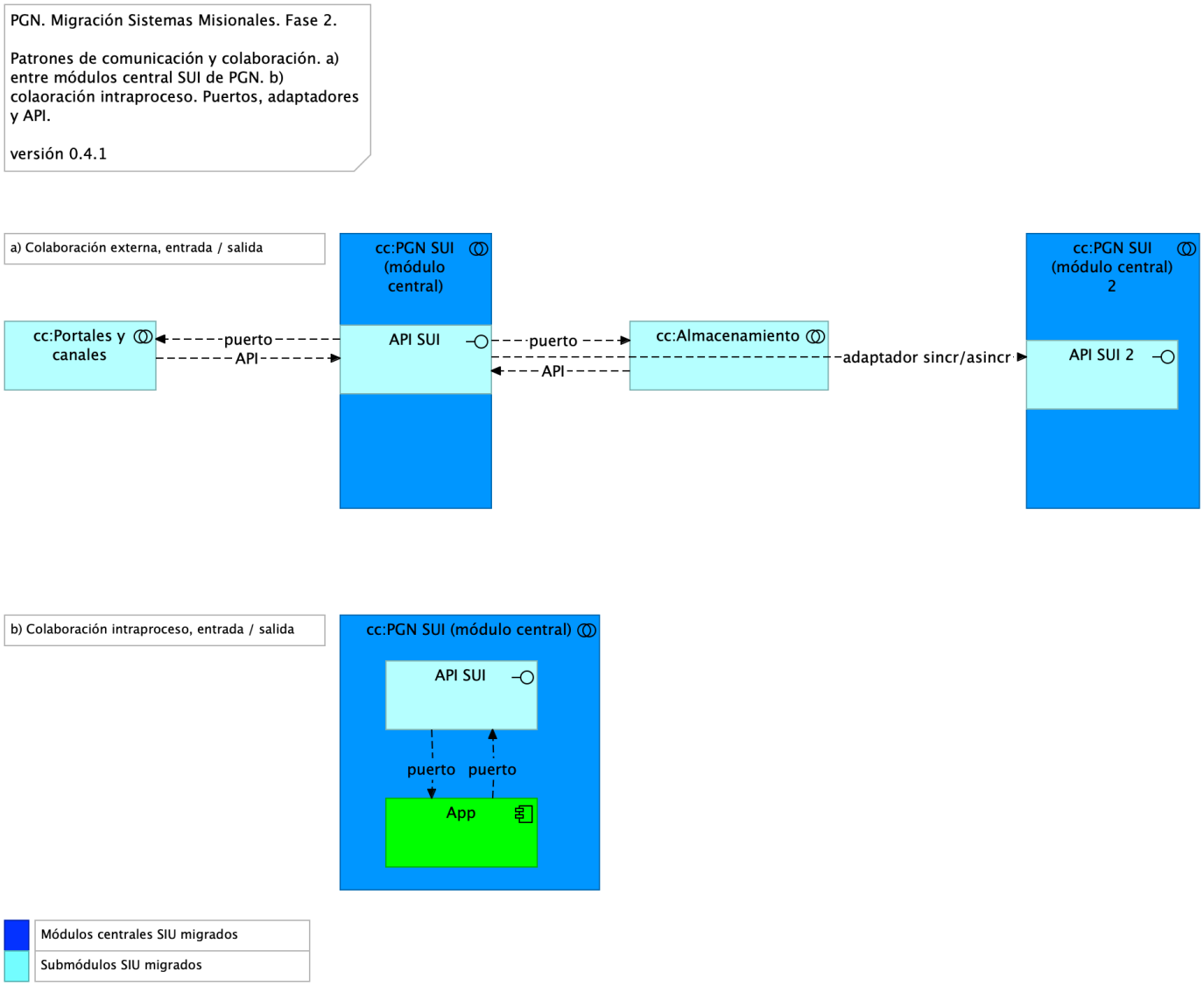


Imagen 8: Vista. Migracion.1c.SIU Módulos Colaboración

Patrón de Distribución y Colaboración estándar para el SUI.

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

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

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

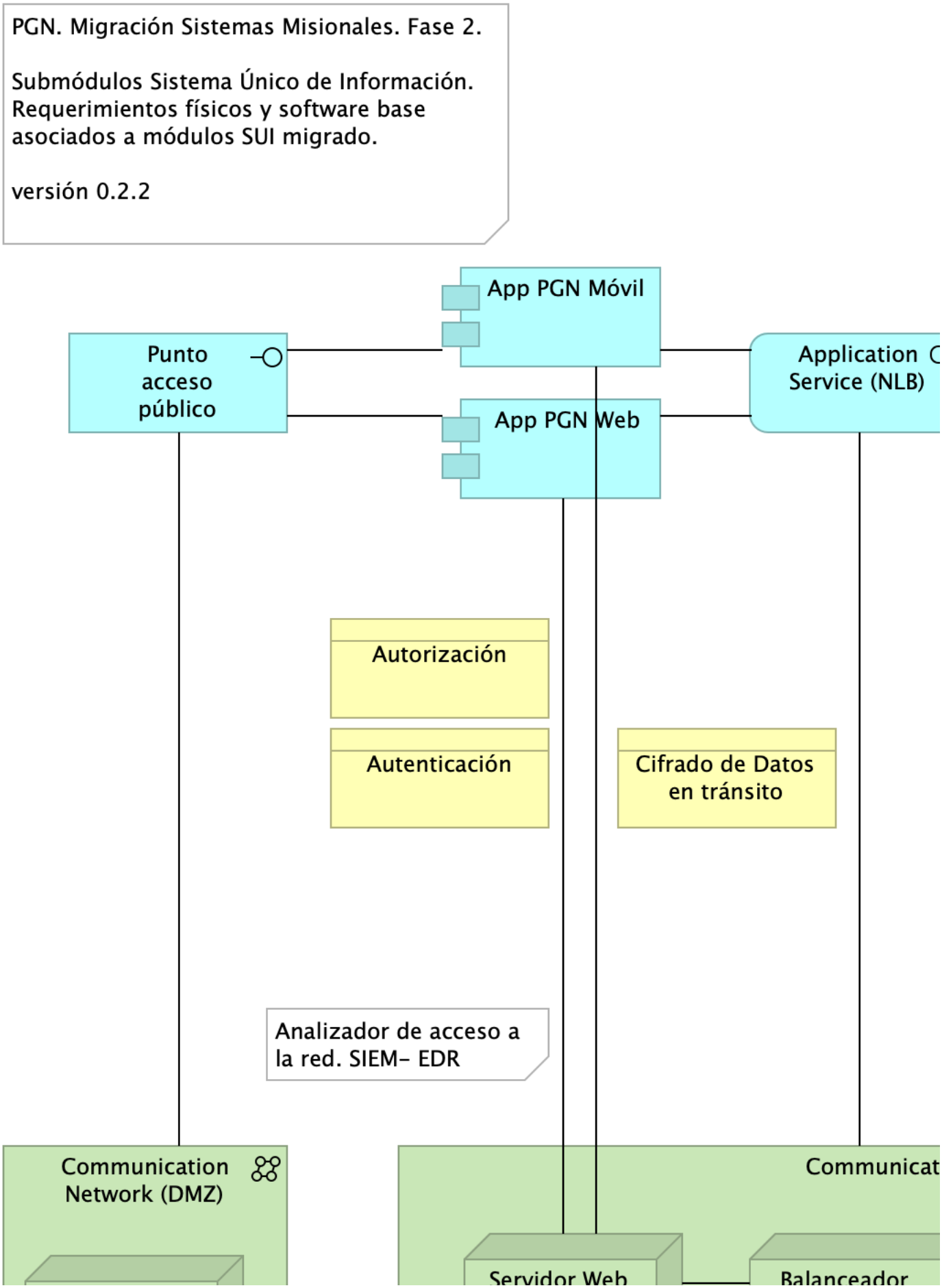
Catálogo de Elementos

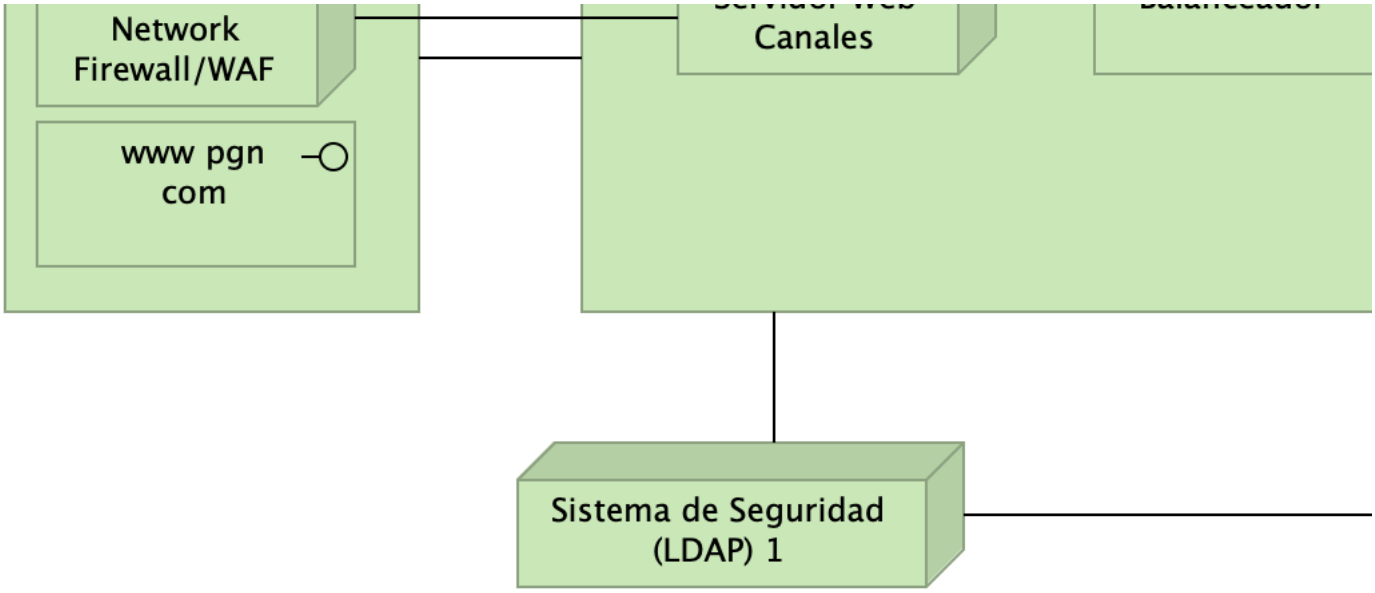
Nombre	Tipo	Descripción	Prop.
cc:Almacenamiento	application-collaboration	Espacio de almacenamiento operativo y transaccional de un módulo central del SUI migrado.	
cc:PGN SUI (módulo central)	application-collaboration	Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular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

Nombre	Tipo	Descripción	Prop.
cc:PGN SUI (módulo central) 2	application-collaboration	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN.	
cc:Portales y canales	application-collaboration	Submódulo de portales internos de la PGN a donde llega el SUI. Interfaz web que usa al SUI para llegar a direcciones y subdirecciones de la PGN. La plataforma principal de portales en este contexto es SharePoint de Microsoft.	
App	application-component		*plataforma:* node Js *brecha:* 100
API SUI	application-interface	API de representación del módulo. Centralización de la comunicación con otros módulos del SUI migrado.	
API SUI	application-interface	API de representación del módulo. Centralización de la comunicación con otros módulos del SUI migrado.	
API SUI 2	application-interface	API de representación del módulo. Centralización de la comunicación con otros módulos del SUI migrado.	

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

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





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

Metodología

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

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

Gestión de identidades y Control de acceso:

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

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

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

REGLAS PARA LA CREACIÓN DE USUARIOS. Identificación de Mecanismos:

En este ítem se deben identificar las herramientas con las que cuenta la entidad, las cuales deberán ser registradas en el documento denominado: “Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_1 (Mecanismos)”. Identificación de Roles y Privilegios Este ítem proporciona al sistema la definición de las políticas organizacionales en cuanto a la definición de los privilegios y roles de los diferentes actores en cada uno de los aplicativos con los que estos interactúan dentro de sus funciones, registradas en el documento denominado: “Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_2 (Roles)”. Aprovisionamiento de cuentas Este ítem establece el proceso adecuado para el aprovisionamiento y des aprovisionamiento de cuentas de usuarios en las diferentes aplicaciones, permitiendo toda la gestión de ellas por medio de un sistema de directorio único y centralizado, Este aprovisionamiento se encuentra registrado en el documento denominado: “Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_4 y Hoja_5 (Permisos)”. Establecimiento de mecanismos de control de acceso:
Este ítem controla que usuarios tienen permitido el acceso a los diferentes aplicativos o herramientas dentro de la organización permitiendo 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)”.

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

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

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

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

Aprovisionamiento de cuentas

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

Establecimiento de mecanismos de control de acceso:
Este ítem controla que usuarios tienen permitido el acceso a los diferentes aplicativos o herramientas dentro de la organización permitiendo 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)”.

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

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

Con el objetivo de incrementar el nivel de seguridad, para el proceso de autenticación se tendrán en cuenta las siguientes consideraciones:

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

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

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

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

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

Bloqueo de cuentas: Aquellas cuentas sobre las que se han 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.

Proteger la información propia de la PGN utilizando mecanismos de cifrado que permita garantizar los pilares de Segurida de la Información Confidencialidad e integridad, asimismo reducir los riesgos de la información mediante la ayuda de Técnicas Criptograficas.

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

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

Como implementar certificados SSL? Podran ser adquiridos a través del proveedor de dominios.

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 envio de la información, proporcionando una autenticación solida, restringiendo la manipulación, interceptación y alteración de mensajes. La ultima versión del TLS es la 1.3

Catálogo de Elementos

Nombre	Tipo	Descripción	Prop.
Application Collaboration	application-collaboration		
Application Collaboration	application-collaboration		
App	application-component		*plataforma:* node Js *brecha:* 100
App PGN Móvil	application-component		*plantilla:* element-md-bold *brecha:* 100
App PGN Web	application-component		*plataforma:* angular 11 *brecha:* 100
Config	application-component		*plataforma:* cs
Punto acceso público	application-interface	URL tipo C HTTP	
Application Service (NLB)	application-service		*plataforma:* angular 11 *brecha:* 100
Interfaz de datos 1	application-service		
Interfaz de datos 2	application-service		
Autenticación	business-object		
Autorización	business-object		
Cifrado de Datos en tránsito	business-object		
Cifrado de datos en tránsito	business-object	Proteger la información propia de la PGN utilizando mecanismos de cifrado que permita garantizar los pilares de Segurida de la Información Confidencialidad e integridad, asimismo reducir los riesgos de la información mediante la ayuda de Técnicas Criptograficas. Como mecanismos se propone implementar estos mecanismos de cifrado, como el protocolo TLS (Transport Layer Security) que permite a dos partes identificarse y autenticarse entre sí y comunicarse con confidencialidad e integridad de datos a partir de la conexión del usuario y un servidor WEB. Se propone integrar certificados SSL, que permite cifrar la información confidencial a fin de que solo los autorizados puedan tener acceso a ella, y asi evitar manipulacion de información confidencial. La Seguridad que brinda SSL, da garantía para acceder a los aplicativos de PNG. Como implementar certificados SSL? Podran ser adquiridos a través del proveedor de dominios. 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 envio de la información, proporcionando una autenticación solida, restringiendo la manipulación, interceptación y alteración de mensajes. La ultima versión del TLS es la 1.3	
Communication Network (DMZ)	communication-network		
Communication Network (LAN)	communication-network		
Communication Network (internet)	communication-network		
Balanceador	node		
Firewall BDD	node		*brecha:* 100
Network Firewall/WAF	node		*brecha:* 100
Servidor BDD App	node	Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz. Discos SO C: 126 GB, Backup E: 511 GB, SQL Data F: 510 GB, SQL Log G: 510 GB, TempDB G: 63.6 GB.	
Servidor BDD Config	node	Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz. Discos SO C: 80 GB, Backup E: 250 GB, SQL Data F: 250 GB, SQL Log G: 250 GB, TempDB G: 30 GB.	
Servidor Web App	node	Windows Server 2019 Standard o Datacenter x64. Nombre físico. IP LAN. IP Pública. Windows Server 2019 Standard or Datacenter x64. RAM 8 GB. CPU 64 Bits. 4 Cores de 2 Ghz. Discos SO C: 126 GB. SO D: 16 GB.	

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

Diagrama de Clases y Componentes de solución

Migracion.1b.1. SIU Módulos Componentes

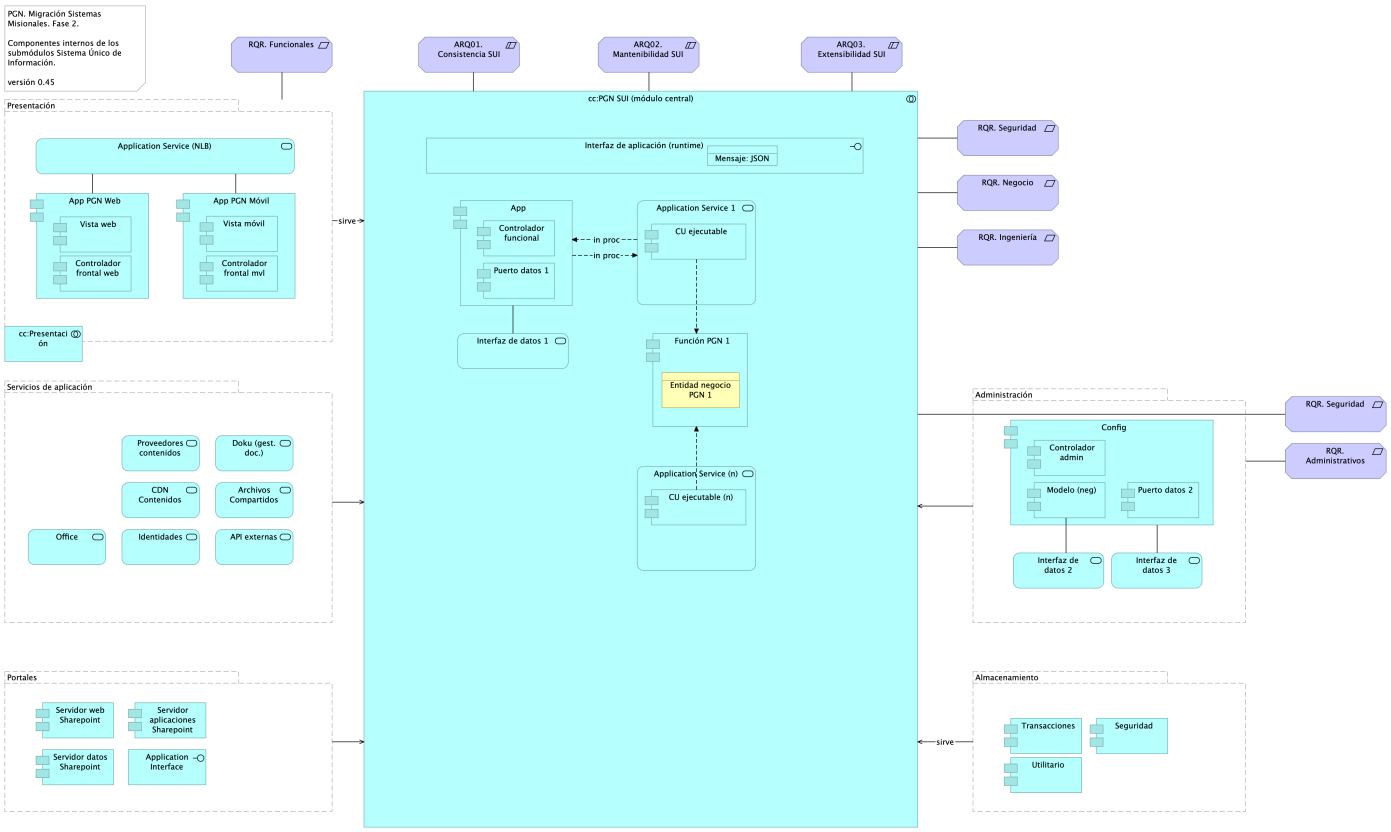


Imagen 9: Vista. Migracion.1b.1. SIU Módulos Componentes

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

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

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

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

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

Consideraciones de Seguridad Vista Web

- Verificados los SSL, se recomienda adquirir SSL seguros, con entidades certificadoras.

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

4. SERVICIOS IDENTIFICADOS: Servidor web: Microsoft-IIS/10.0 Marco de Programación: ASP.NET Huellas digitales identificadas: Huella digital SHA-256 "FC:79:06:7E:F5:24:20:50:F1:C0:74:F7:85:56:B9:05:B7:33:A3:2D:44:A0:48" Huella digital SHA1 "8C:48:BD:E2:F5:18:18:C3:85:96:68:44:2E:28:A0:68:08:2F:0A:BE"

Catálogo de Elementos

Nombre	Tipo	Descripción	Prop.
cc:PGN SUI (módulo central)	application-collaboration	Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular de la PGN.	
cc:Presentación	application-collaboration	Submódulo de presentación del SUI. interfaz gráfica, interfaz web visible a los usuarios clientes y funcionarios de la PGN.	

Nombre	Tipo	Descripción	Prop.
App	application-component		*plataforma:* node Js *brecha:* 100
App PGN Móvil	application-component		*plantilla:* element-md-bold *brecha:* 100
App PGN Web	application-component		*plataforma:* angular 11 *brecha:* 100
CU ejecutable	application-component		*plataforma:* js
CU ejecutable (n)	application-component		*plataforma:* js
Config	application-component		*plataforma:* cs
Controlador admin	application-component		*plataforma:* cs
Controlador frontal mvl	application-component		*plataforma:* js
Controlador frontal web	application-component	- Verificados los SSL, se recomienda adquirir SSL seguros, con entidades certificadoras. Si se desea continuar con SSL de Let's Encrypt, se recomienda automatizar el proceso de actualización dado que al dejar estos en modo actualización manual es probable el olvido de esta actualización (Estos certificados se deben actualizar trimestralmente y no cuentan con las características de seguridad necesarias.	*plataforma:* js
Controlador funcional	application-component		*plataforma:* js
Función PGN 1	application-component	La unidad de cómputo que resulta en la aplicación de una regla de negocio.	*plataforma:* js
Modelo (neg)	application-component		*plataforma:* cs
Puerto datos 1	application-component		*plataforma:* js
Puerto datos 2	application-component		*plataforma:* cs
Seguridad	application-component		*plataforma:* sql *brecha:* 100
Servidor aplicaciones Sharepoint	application-component		
Servidor datos Sharepoint	application-component		
Servidor web Sharepoint	application-component		
Transacciones	application-component		*plataforma:* sql *brecha:* 100
Utilitario	application-component		*plataforma:* no-sql
Vista móvil	application-component		*plataforma:* js
Vista web	application-component		*plataforma:* html
Application Interface	application-interface		
Interfaz de aplicación (runtime)	application-interface	Servidor web: Microsoft-IIS/10.0 Marco de Programación: ASP.NET Huellas digitales identificadas: Huella digital SHA-256 "FC:79:06:7E:F5:24:20:50:F1:C0:74:F7:85:56:B9:05:B7:33:A3:2D:44:A0:48" Huella digital SHA1 "8C:48:BD:E2:F5:18:18:C3:85:96:68:44:2E:28:A0:68:08:2F:0A:BE"	*plataforma:* angular 11
API externas	application-service		
Application Service (NLB)	application-service		*plataforma:* angular 11 *brecha:* 100
Application Service (n)	application-service	Implementación de un caso de uso de negocio, independiente y demostrable. Contiene a la unidad ejecutable del CU y a la entidad	
Application Service 1	application-service	Implementación de un caso de uso de negocio, independiente y demostrable. Contiene a la unidad ejecutable del CU y reutiliza (accede a) una entidad de negocio, que puede ser también una función PGN.	
Archivos Compartidos	application-service		
CDN Contenidos	application-service		*brecha:* 100
Doku (gest. doc.)	application-service		*brecha:* 100
Identidades	application-service		
Interfaz de datos 1	application-service		
Interfaz de datos 2	application-service		
Interfaz de datos 3	application-service		
Office	application-service		

Nombre	Tipo	Descripción	Prop.
Proveedores contenidos	application-service		*brecha:* 100
Entidad negocio PGN 1	business-object	Repreesnta un objeto de negocio del contexto de la entidad PGN,, por ejemplo: un decreto, una intervención, una conciliación.	
ARQ01. Consistencia SUI	constraint	Unifica las entidades de negocio PGN, entre las que se incluyen a conciliaciones, publicaciones de relatoría, resoluciones, en artefactos reutilizables. Distinto de que estas entidades (y su lógica de negocio) estén dispersos entre los sistemas del SUI, estarán concentradas en un único artefacto correspondiente. Calidad sistémica: la consistencia persigue que el resultado de la lógica de negocio sea la misma entre los módulos del SUI migrado. Esto redunda a mantenibilidad y gestión: tiende a tener un solo punto de cambio y dificulta la transferencia de dependencias implícitas a otros procesos.	
ARQ02. Mantenibilidad SUI	constraint	Evitar las dependencia transitivas de los módulos misionales del SUI a componentes y sistemas de terceros o submódulos no misionales. Calidad sistémica: la mantenibilidad por control de dependencias que optimiza el diseño Migración SUI está dada por el control de cambios no programados sobre los componentes misionales del SUI (corrupción de componentes). Ver Patrón de Diseño Migración SUI, más adelante en el documento.	
ARQ03. Extensibilidad SUI	constraint	Concentración de los componentes de negocio, misionales, del SUI protegidos de cambios provenientes de otros sistemas. Ver Patrón de Diseño Migración SUI, más adelante en el documento. Calidad sistémica: la extensibilidad que optimiza el diseño Migración SUI está dada por el intercambio de submódulos no misionales, como el gestor documental, sin afectación de los componentes misionales que este diseño protege.	
Mensaje: JSON	data-object		
Administración	grouping		
Almacenamiento	grouping		
Portales	grouping	Submódulo de portales internos de la PGN a donde llega el SUI. Interfaz web que usa al SUI para llegar a direcciones y subdirecciones de la PGN. La plataforma principal de portales en este contexto es Sharepoint de Microsoft.	
Presentación	grouping	Submódulo de presentación del SUI. interfaz gráfica, interfaz web visible a los usuarios clientes y funcionarios de la PGN.	
Servicios de aplicación	grouping	Submódulo de servicios utilitarios que sirven al SUI. Servicios variados que cumplen roles facilitadores de las actividades misionales del SUI. Ejemplos de estos servicios son los de gestión documental, implementado por Doku en el contexto de PGN.	
RQR. Administrativos	requirement		
RQR. Funcionales	requirement		
RQR. Ingeniería	requirement		
RQR. Negocio	requirement		
RQR. Seguridad	requirement	Requerimientos de seguridad, SUI, Migración, en aspectos de comunicación, autenticación, autorización y (manejo de) sesiones.	
RQR. Seguridad	requirement	Requerimientos de seguridad, SUI, Migración, en aspectos de comunicación, autenticación, autorización y (manejo de) sesiones.	

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

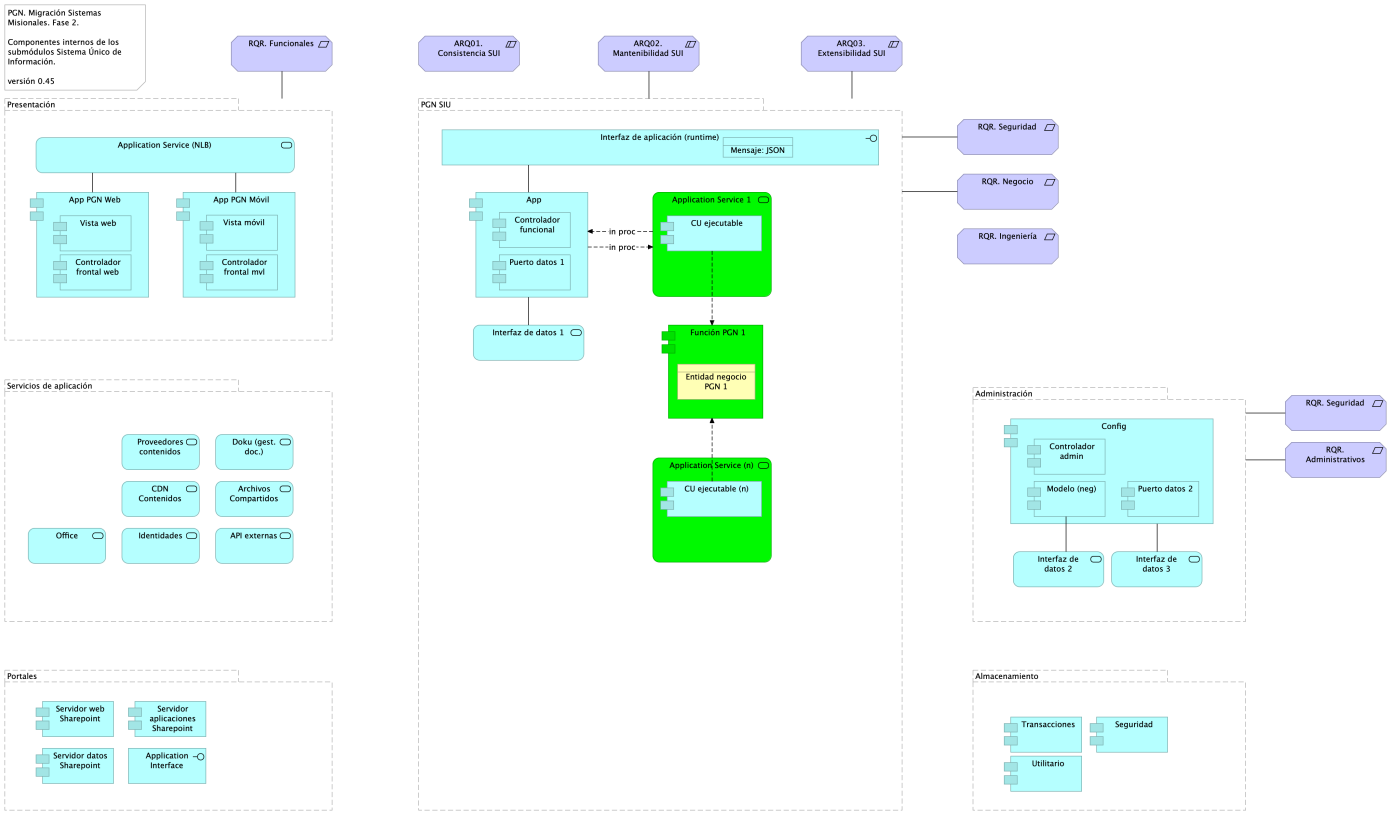


Imagen 10: Vista. Migracion.1b.2. SIU Módulos Componentes. Brecha

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

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

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

Catálogo de Elementos

Nombre	Tipo	Descripción	Prop.
App	application-component		*plataforma:* node Js *brecha:* 100
App PGN Móvil	application-component		*plantilla:* element-md-bold *brecha:* 100
App PGN Web	application-component		*plataforma:* angular 11 *brecha:* 100
CU ejecutable	application-component		*plataforma:* js
CU ejecutable (n)	application-component		*plataforma:* js
Config	application-component		*plataforma:* cs
Controlador admin	application-component		*plataforma:* cs
Controlador frontal mvl	application-component		*plataforma:* js
Controlador frontal web	application-component	- Verificados los SSL, se recomienda adquirir SSL seguros, con entidades certificadoras. Si se desea continuar con SSL de Let's Encrypt, se recomienda automatizar el proceso de actualización dado que al dejar estos en modo actualización manual es probable el olvido de esta actualización (Estos certificados se deben actualizar trimestralmente y no cuentan con las características de seguridad necesarias.	*plataforma:* js
Controlador funcional	application-component		*plataforma:* js
Función PGN 1	application-component	La unidad de cómputo que resulta en la aplicación de una regla de negocio.	*plataforma:* js
Modelo (neg)	application-component		*plataforma:* cs
Puerto datos 1	application-component		*plataforma:* js
Puerto datos 2	application-component		*plataforma:* cs

Nombre	Tipo	Descripción	Prop.
Seguridad	application-component		*plataforma:* sql *brecha:* 100
Servidor aplicaciones Sharepoint	application-component		
Servidor datos Sharepoint	application-component		
Servidor web Sharepoint	application-component		
Transacciones	application-component		*plataforma:* sql *brecha:* 100
Utilitario	application-component		*plataforma:* no-sql
Vista móvil	application-component		*plataforma:* js
Vista web	application-component		*plataforma:* html
Application Interface	application-interface		
Interfaz de aplicación (runtime)	application-interface	Servidor web: Microsoft-IIS/10.0 Marco de Programación: ASP.NET Huellas digitales identificadas: Huella digital SHA-256 “FC:79:06:7E:F5:24:20:50:F1:C0:74:F7:85:56:B9:05:B7:33:A3:2D:44:A0:48” Huella digital SHA1 “8C:48:BD:E2:F5:18:18:C3:85:96:68:44:2E:28:A0:68:08:2F:0A:BE”	*plataforma:* angular 11
API externas	application-service		
Application Service (NLB)	application-service		*plataforma:* angular 11 *brecha:* 100
Application Service (n)	application-service	Implementación de un caso de uso de negocio, independiente y demostrable. Contiene a la unidad ejecutable del CU y a la entidad	
Application Service 1	application-service	Implementación de un caso de uso de negocio, independiente y demostrable. Contiene a la unidad ejecutable del CU y reutiliza (accede a) una entidad de negocio, que puede ser también una función PGN.	
Archivos Compartidos	application-service		
CDN Contenidos	application-service		*brecha:* 100
Doku (gest. doc.)	application-service		*brecha:* 100
Identidades	application-service		
Interfaz de datos 1	application-service		
Interfaz de datos 2	application-service		
Interfaz de datos 3	application-service		
Office	application-service		
Proveedores contenidos	application-service		*brecha:* 100
Entidad negocio PGN 1	business-object	Repreesnta un objeto de negocio del contexto de la entidad PGN,, por ejemplo: un decreto, una intervención, una conciliación.	
ARQ01. Consistencia SUI	constraint	Unifica las entidades de negocio PGN, entre las que se incluyen a conciliaciones, publicaciones de relatoría, resoluciones, en artefactos reutilizables. Distinto de que estas entidades (y su lógica de negocio) estén dispersos entre los sistemas del SUI, estarán concentradas en un único artefacto correspondiente. Calidad sistémica: la consistencia persigue que el resultado de la lógica de negocio sea la misma entre los módulos del SUI migrado. Esto redunda a mantenibilidad y gestión: tiende a tener un solo punto de cambio y dificulta la transferencia de dependencias implícitas a otros procesos.	
ARQ02. Mantenibilidad SUI	constraint	Evitar las dependencia transitivas de los módulos misionales del SUI a componentes y sistemas de terceros o submódulos no misionales. Calidad sistémica: la mantenibilidad por control de dependencias que optimiza el diseño Migración SUI está dada por el control de cambios no programados sobre los componentes misionales del SUI (corrupción de componentes). Ver Patrón de Diseño Migración SUI, más adelante en el documento.	

Nombre	Tipo	Descripción	Prop.
ARQ03. Extensibilidad SUI	constraint	Concentración de los componentes de negocio, misionales, del SUI protegidos de cambios provenientes de otros sistemas. Ver Patrón de Diseño Migración SUI, más adelante en el documento. Calidad sistémica: la extensibilidad que optimiza el diseño Migración SUI está dada por el intercambio de submódulos no misionales, como el gestor documental, sin afectación de los componentes misionales que este diseño protege.	
Mensaje: JSON	data-object		
Administración	grouping		
Almacenamiento	grouping		
PGN SIU	grouping	El objetivo principal de la arquitectura del SUI de la migración es la centralización de los conceptos misionales: concentrar los conceptos misionales en componentes aislados; dejar por fuera de estos componentes misionales todo lo distintos a la misionalidad de la PGN. Los objetivos secundarios de esta arquitectura SUI de la migración son flexibilidad y extensibilidad. Dichos objetivos son independientes. Es decir, estos pueden ser maximizados sin conclifcto entre ellos. El API transaccional construida en Node js con ORM Sequelize cuenta con obligatoriedad de token tipo bearer generado desde Api config (Api security token generado con autenticación de directorio activo o login de usuario externo) cuenta con un modelo de capas donde primero se encuentra un DTO consistente en estructura de datos y métodos de “check permissions” (un endpoint del api de seguridad para validar privilegios sobre las acciones de la petición en ingreso) luego dependiendo del tipo de transacción se tiene una capa para Lappiz functions, Lappiz Jobs (Tareas programables) y Lappiz model (Generado con base ORM sequelize). Todas las transacciones una vez son validadas en token y permisos, pasan a un tenedor de conexión para modificar las cadenas de conexión en marcha y saber que usuario de bd va a efectuar la operación y con qué privilegios. Todas las peticiones entran en un modelo natural de node js compuesto por un Event queue y un evento Loop; estas peticiones se procesan en la base de datos y todas las excepciones controladas se registran en un log de errores en formato txt con las especificaciones y devolviendo errores controlados con protocolos HTTPs al Runtime (front de SUI).	
Portales	grouping	Submódulo de portales internos de la PGN a donde llega el SUI. Interfaz web que usa al SUI para llegar a direcciones y subdirecciones de la PGN. La plataforma principal de portales en este contexto es Sharepoint de Microsoft.	
Presentación	grouping	Submódulo de presentación del SUI. interfaz gráfica, interfaz web visible a los usuarios clientes y funcionarios de la PGN.	
Servicios de aplicación	grouping	Submódulo de servicios utilitarios que sirven al SUI. Servicios variados que cumplen roles facilitadores de las actividades misionales del SUI. Ejemplos de estos servicios son los de gestión documental, implementado por Doku en el contexto de PGN.	
RQR. Administrativos	requirement		
RQR. Funcionales	requirement		
RQR. Ingeniería	requirement		
RQR. Negocio	requirement		
RQR. Seguridad	requirement	Requerimientos de seguridad, SUI, Migración, en aspectos de comunicación, autenticación, autorización y (manejo de) sesiones.	

Nombre	Tipo	Descripción	Prop.
RQR. Seguridad	requirement	Requerimientos de seguridad, SUI, Migración, en aspectos de comunicación, autenticación, autorización y (manejo de) sesiones.	

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

Migracion.4. CI

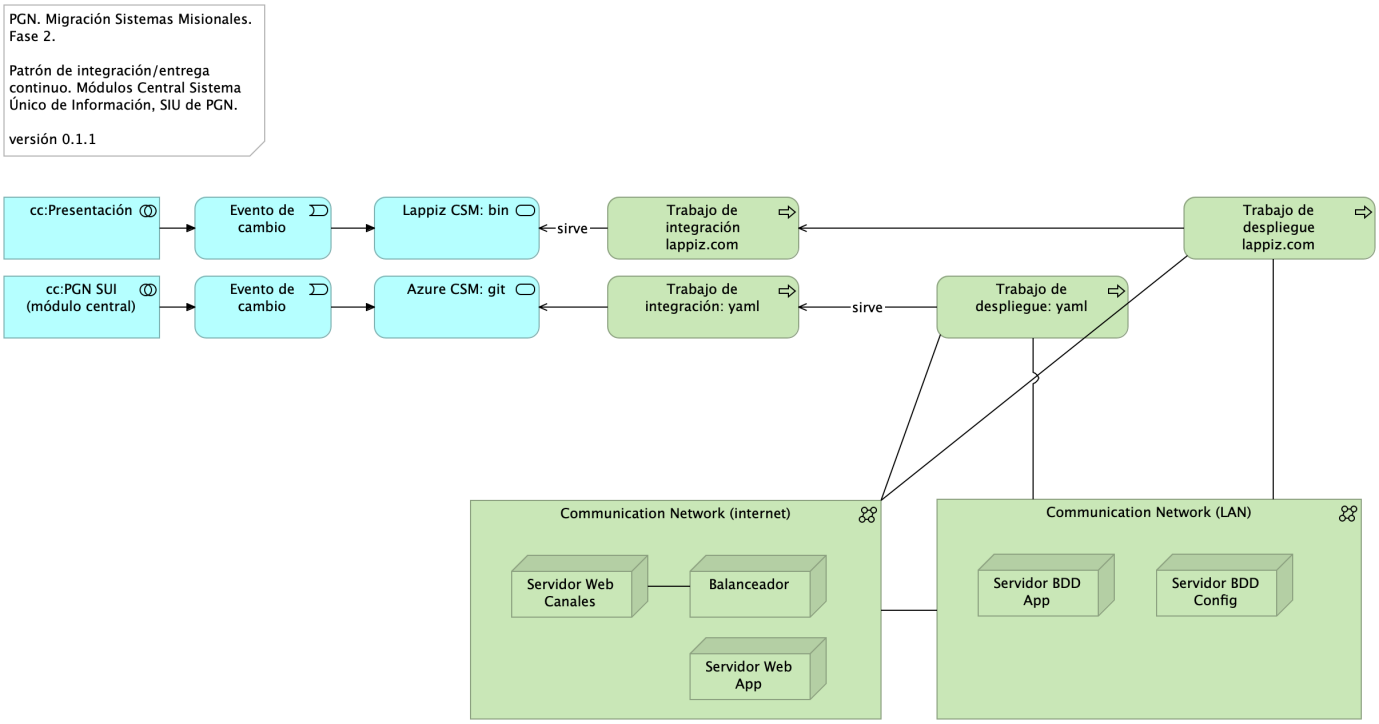


Imagen 11: Vista. Migracion.4. CI

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

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

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

Catálogo de Elementos

Nombre	Tipo	Descripción	Prop.
cc:PGN SUI (módulo central)	application-collaboration	Módulo central SUI migrado. Módulo independiente y asignado a un dominio partigular de la PGN.	
cc:Presentación	application-collaboration	Submódulo de presentación del SUI. interfaz gráfica, interfaz web visible a los usuarios clientes y funcionarios de la PGN.	
Evento de cambio	application-event		
Evento de cambio	application-event		
Azure CSM: git	application-service		
Lappiz CSM: bin	application-service		
Communication Network (LAN)	communication-network		
Communication Network (internet)	communication-network		
Balanceador	node		
Servidor BDD App	node	Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz. Discos SO C: 126 GB, Backup E: 511 GB, SQL Data F: 510 GB, SQL Log G: 510 GB, TempDB G: 63.6 GB.	
Servidor BDD Config	node	Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz. Discos SO C: 80 GB, Backup E: 250 GB, SQL Data F: 250 GB, SQL Log G: 250 GB, TempDB G: 30 GB.	

Nombre	Tipo	Descripción	Prop.
Servidor Web App	node	Windows Server 2019 Standard o Datacenter x64. Nombre físico. IP LAN. IP Pública. Windows Server 2019 Standard or Datacenter x64. RAM 8 GB. CPU 64 Bits. 4 Cores de 2 Ghz. Discos SO C: 126 GB. SO D: 16 GB.	
Servidor Web Canales	node	Windows Server 2019 Standard o Datacenter x64. Nombre físico. IP LAN. IP Pública. Windows Server 2019 Standard or Datacenter x64. RAM 8 GB. CPU 64 Bits. 4 Cores de 2 Ghz. Discos SO C: 126 GB. SO D: 16 GB.	
Trabajo de despliegue lappiz.com	technology-process		
Trabajo de despliegue: yaml	technology-process		
Trabajo de integración lappiz.com	technology-process		
Trabajo de integración: yaml	technology-process		

Documento de Relación de Tecnologías y Licenciamiento

Migracion.5. Licenciamiento

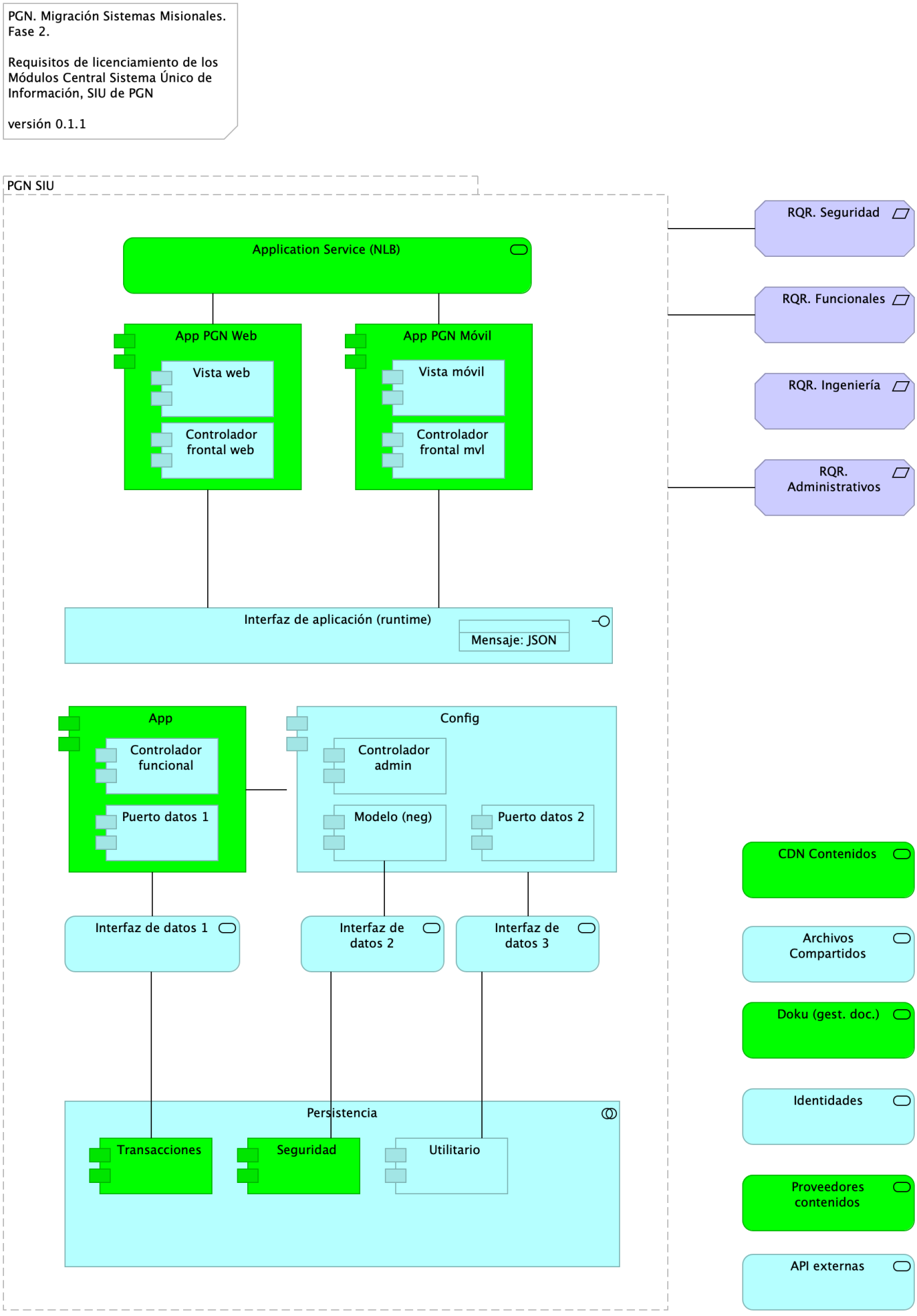


Imagen 12: Vista. Migracion.5. Licenciamiento

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

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

Catálogo de Elementos

Nombre	Tipo	Descripción	Prop.
Persistencia	application-collaboration		
App	application-component		*plataforma:* node Js *brecha:* 100
App PGN Móvil	application-component		*plantilla:* element-md-bold *brecha:* 100
App PGN Web	application-component		*plataforma:* angular 11 *brecha:* 100
Config	application-component		*plataforma:* cs
Controlador admin	application-component		*plataforma:* cs
Controlador frontal mvl	application-component		*plataforma:* js
Controlador frontal web	application-component	- Verificados los SSL, se recomienda adquirir SSL seguros, con entidades certificadoras. Si se desea continuar con SSL de Let's Encrypt, se recomienda automatizar el proceso de actualización dado que al dejar estos en modo actualización manual es probable el olvido de esta actualización (Estos certificados se deben actualizar trimestralmente y no cuentan con las características de seguridad necesarias.	*plataforma:* js
Controlador funcional	application-component		*plataforma:* js
Modelo (neg)	application-component		*plataforma:* cs
Puerto datos 1	application-component		*plataforma:* js
Puerto datos 2	application-component		*plataforma:* cs
Seguridad	application-component		*plataforma:* sql *brecha:* 100
Transacciones	application-component		*plataforma:* sql *brecha:* 100
Utilitario	application-component		*plataforma:* no-sql
Vista móvil	application-component		*plataforma:* js
Vista web	application-component		*plataforma:* html
Interfaz de aplicación (runtime)	application-interface	Servidor web: Microsoft-IIS/10.0 Marco de Programación: ASP.NET Huellas digitales identificadas: Huella digital SHA-256 "FC:79:06:7E:F5:24:20:50:F1:C0:74:F7:85:56:B9:05:B7:33:A3:2D:44:A0:48" Huella digital SHA1 "8C:48:BD:E2:F5:18:18:C3:85:96:68:44:2E:28:A0:68:08:2F:0A:BE"	*plataforma:* angular 11
API externas	application-service		
Application Service (NLB)	application-service		*plataforma:* angular 11 *brecha:* 100
Archivos Compartidos	application-service		
CDN Contenidos	application-service		*brecha:* 100
Doku (gest. doc.)	application-service		*brecha:* 100
Identidades	application-service		
Interfaz de datos 1	application-service		
Interfaz de datos 2	application-service		
Interfaz de datos 3	application-service		
Proveedores contenidos	application-service		*brecha:* 100
Mensaje: JSON	data-object		

Nombre	Tipo	Descripción	Prop.
PGN SIU	grouping	El objetivo principal de la arquitectura del SUI de la migración es la centralización de los conceptos misionales: concentrar los conceptos misionales en componentes aislados; dejar por fuera de estos componentes misionales todo lo distintos a la misionalidad de la PGN. Los objetivos secundarios de esta arquitectura SUI de la migración son flexibilidad y extensibilidad. Dichos objetivos son independientes. Es decir, estos pueden ser maximizados sin conclifcto entre ellos. El API transaccional construida en Node js con ORM Sequelize cuenta con obligatoriedad de token tipo bearer generado desde Api config (Api security token generado con autenticación de directorio activo o login de usuario externo) cuenta con un modelo de capas donde primero se encuentra un DTO consistente en estructura de datos y métodos de "check permissions" (un endpoint del api de seguridad para validar privilegios sobre las acciones de la petición en ingreso) luego dependiendo del tipo de transacción se tiene una capa para Lappiz functions, Lappiz Jobs (Tareas programables) y Lappiz model (Generado con base ORM sequelize). Todas las transacciones una vez son validadas en token y permisos, pasan a un tenedor de conexión para modificar las cadenas de conexión en marcha y saber que usuario de bd va a efectuar la operación y con qué privilegios. Todas las peticiones entran en un modelo natural de node js compuesto por un Event queue y un evento Loop; estas peticiones se procesan en la base de datos y todas las excepciones controladas se registran en un log de errores en formato txt con las especificaciones y devolviendo errores controlados con protocolos HTTPs al Runtime (front de SUI).	
RQR. Administrativos	requirement		
RQR. Funcionales	requirement		
RQR. Ingeniería	requirement		
RQR. Seguridad	requirement	Requerimientos de seguridad, SUI, Migración, en aspectos de comunicación, autenticación, autorización y (manejo de) sesiones.	

Módulos Requerimientos de Seguridad

Seguridad.Autenticación

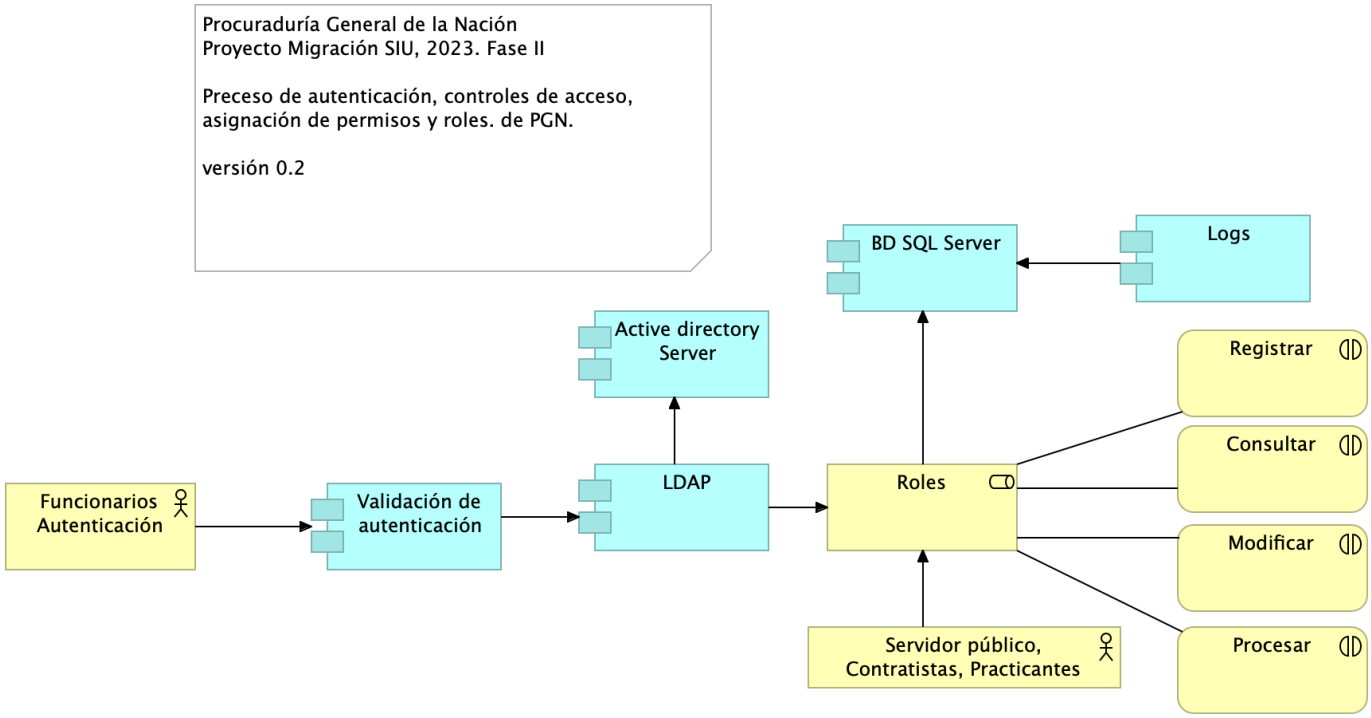


Imagen 13: Vista. Seguridad.Autenticación

Autenticación: Con el objetivo de incrementar el nivel de seguridad, para el proceso de autenticación se tendrán en cuenta las siguientes consideraciones:

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

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

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

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

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

Bloqueo de cuentas: Aquellas cuentas sobre las que se han 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.

La autenticación en el sistema de información comprende un Login de acceso contra Api config (Api Rest .Net Framework) y Active Directory. La misma api de configuración reconoce si el usuario es interno o externo (Es decir desde los usuarios el sistema conoce si debe hacer autenticación por directorio activo o en su defecto oAuth)

Catálogo de Elementos

Nombre	Tipo	Descripción	Prop.

Nombre	Tipo	Descripción	Prop.
Active directory Server	application-component	Los tipos de autenticación realizadas a partir de las identidades administradas de los recursos de Azure, entidades de Servicio y Certificados, podrán ser integrado con los dominios del directorio activo (DA) local. Por lo que respecta a la autenticación, será generado con la asignación de usuarios y credenciales definidas alineadas con la política Específica de Control de Acceso., a partir de la integración será validado el ingreso a las diferentes soluciones y/o sistemas de información de la PGN.	
BD SQL Server	application-component	Los datos estarán procesados y almacenados en las bases de datos, el cual tendra implementados mecanismos de seguridad para el cifrado de los datos.	
LDAP	application-component	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).	
Logs	application-component	Registro de actividades que permitirá mantener trazabilidad a partir de los registros de auditoría que contenga 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.	
Validación de autenticación	application-component	Autenticación: Con el objetivo de incrementar el nivel de seguridad, para el proceso de autenticación se tendrán que realizar las diferentes validaciones para el accesos a las soluciones desarrolladas. Caracteristicas de contraseñas: Las contraseñas deberán exigir caracteristicas especiales como mínimo ocho (8) caraceteres, numeros, simbolos, letras mayusculas y minusculas. La aplicación al estar integrada con el directorio activo deberá validar las caracteristicas requeridas, estará en la capacidad de aceptar o rechazar la contraseña. Bloqueo de contraseña: El sistema incluirá controles de bloqueo de cuenta después de un maximo de cinco (5) intentos errados, con el fin de evitar ataques por fuerza bruta. Como la aplicación estará integrada con el directorio activo, este será encargado de definir los números de intentos permitidos antes de bloquear la contraseña de los usuarios. Cierre de Sesión Después de diez (10) minutos de inactividad el sistema deberá cerrar la sesión de trabajo.	
Funcionarios Autenticación	business-actor	Verificación que se realiza con la identidad del Servidor público, Contratista, Aprendiz y/o practicante de la entidad, proceso que se lleva a cabo cuando se ingresa al sistema, a la red o a cualquier base de datos. 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, que definirá la complejidad para la administración de contraseñas (Conjunto de caracteres variado con minúsculas, mayúsculas y números, entre otros). Se deberá permitir para la gestion de usuarios, acciones como (creación, suministros de accesos, asignación de privilegios, revocatoria de accesos, etc), roles y perfiles, grupos de usuarios, asociacion de acciones para cada rol, y la administración exclusiva de los administradores del sistema de Información.	

Nombre	Tipo	Descripción	Prop.
Servidor público, Contratistas, Practicantes y/o aprendices.	business-actor	Persona natural que hacee parte la Procuraduría General de la Nación.	
Consultar	business-interaction	Permitirá identificar los Servidores públicos, Contratistas, Practicantes y/o aprendices que podran Consultar informacion sobre las diferentes soluciones.	
Modificar	business-interaction	Permitirá identificar los Servidores públicos, Contratistas, Practicantes y/o aprendices que tendrán acceso a modificar/ Actualizar informacion sobre las diferentes soluciones.	
Procesar	business-interaction	Permitirá identificar los Servidores públicos, Contratistas, Practicantes y/o aprendices que podran inactivar información sobre los diferentes sistemas de información.	
Registrar	business-interaction	Permitirá definir los Servidores públicos, Contratistas, Practicantes y/o aprendices que podran registrar informacion sobre las diferentes soluciones.	
Roles	business-role	Se definirán los roles y perfiles para acceder a los diferentes módulos de las soluciones desarrolladas.	

Seguridad.Autorización

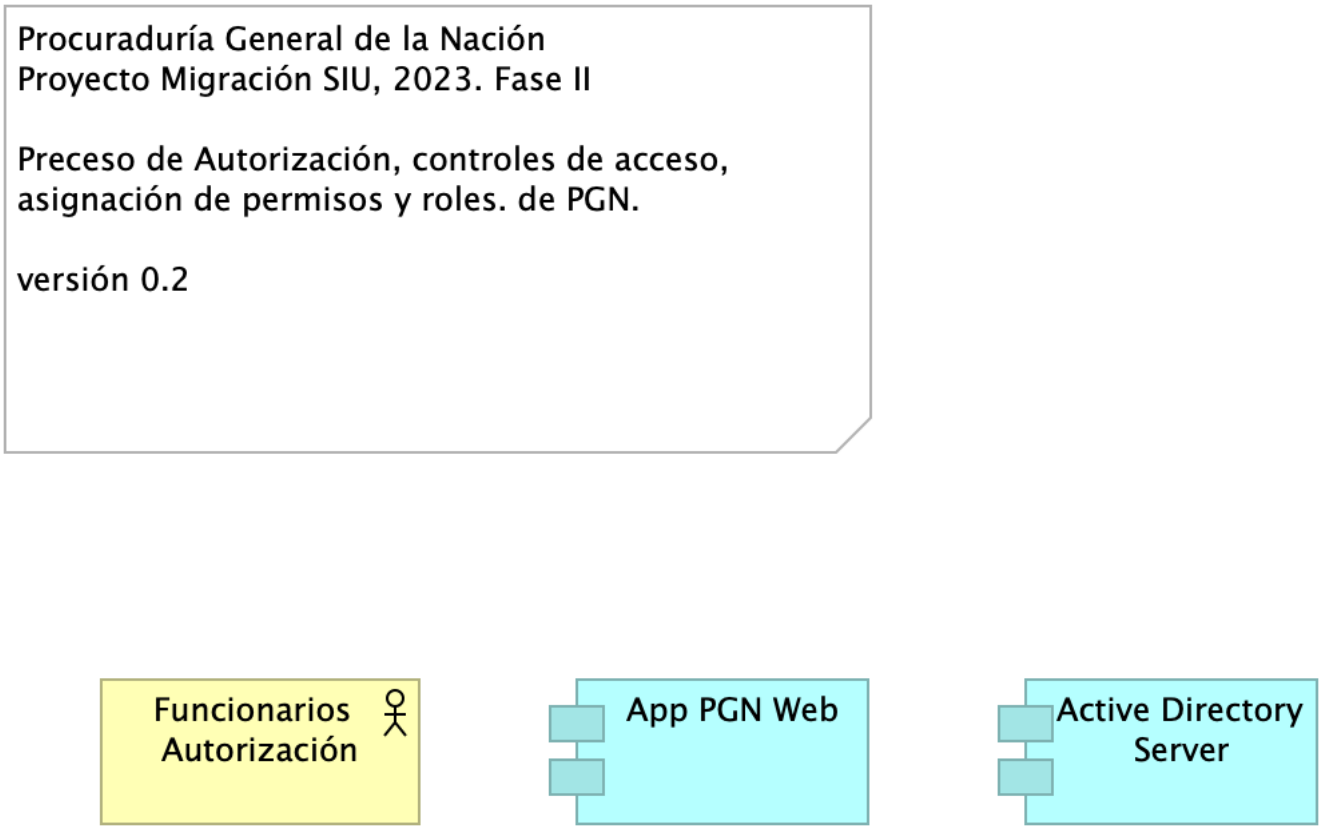


Imagen 14: Vista. Seguridad.Autorización

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

Un proceso de autorización basado en roles, identifica tres factores importantes, i) Todos los servidores públicos, contratistas, terceros y otros Colaboradores, deben tener un rol asignado, si no es asignado no podrá realizar ninguna acción relacionada con el acceso, ii) un usuario podrá hacer uso de los permisos asociados a los roles asignados, el cual deberá realizar el inicio de sesión el usuario asignado del Directorio activo (DA), iii) los servidores

públicos, contratistas, terceros y otros, solo podrán realizar acciones para las cuales han sido autorizados por medio de la activación de sus roles y/o perfiles.
EL control definido para los accesos basados en roles RBAC, permitirá que solo las personas autorizadas de la PGN podrán acceder a ciertos recursos (programas, equipos, aplicaciones, bases de datos, etc.) definido por sus funciones laborales, lo que permitirá controlar los accesos desde diferentes escenarios: Sistemas de información, redes y aplicaciones.

Para consumo de Api Tx (Api rest node js) se cuenta con peticiones por métodos POST, PATCH, PUT, DELETE, esta no admite transacciones GET y siempre es requerido un bearer token y un sequelize model para garantizar transacciones exitosas.

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

Gestor de roles: La asignación de roles es sincronizada con la identidad de usuario en el servidor de dominio. Para esta gestión se crean las reglas y condiciones que determinan si un usuario puede o no pertenecer a un rol definido por la entidad. Para el gobierno y gestión de identidades y de acceso, se identificó como primera medida la implementación de la siguiente metodología.

2.3.3. Identificación de Mecanismos:

En este ítem se deben identificar las herramientas con las que cuenta la entidad, las cuales deberán ser registradas en el documento denominado: “Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_1 (Mecanismos)”. 2.3.4. Identificación de Roles y Privilegios Este ítem proporciona al sistema la definición de las políticas organizacionales en cuanto a la definición de los privilegios y roles de los diferentes actores en cada uno de los aplicativos con los que estos interactúan dentro de sus funciones, registradas en el documento denominado: “Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_2 (Roles)”.

2.3.5. Aprovisionamiento de cuentas

Este ítem establece el proceso adecuado para el aprovisionamiento y des aprovisionamiento de cuentas de usuarios en las diferentes aplicaciones, permitiendo toda la gestión de ellas por medio de un sistema de directorio único y centralizado, Este aprovisionamiento se encuentra registrado en el documento denominado: “Clasificación y gestión de usuarios, roles y perfiles.xlsx / Hoja_4 y Hoja_5 (Permisos)”. 2.3.6. Establecimiento de mecanismos de control de acceso: Este ítem controla que usuarios tienen permitido el acceso a los diferentes aplicativos o herramientas dentro de la organización permitiendo 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)”. 1.4.6. Definición de Privilegios y accesos. Los accesos y privilegios serán identificados en la matriz, encargado identificar cada uno de los roles y perfiles que se tendrá cada usuario hacia los sistemas de información cumpliendo con el principio del menor privilegio, teniendo en cuenta que los usuarios deberán tener exclusivamente los permisos y privilegios que necesita para el desarrollo de sus actividades. La matriz identificará i) los roles que se deben crear para cada sistema de información, ii) los privilegios que requiere cada rol del sistema y iii) los niveles de accesos requeridos, (Consultar, Modificar, Eliminar) (CRUD) y iv) Tipos de usuarios, roles que pueden ser asignados al perfil, entre otros. 1.4.7. Configuración de permisos La configuración con de los perfiles con sus accesos y privilegios en los sistemas de información se debe realizar empleando las herramientas propias de la procuraduría general de la nacional PGN, y serán asignados los permisos según la matriz de roles y permisos.

Catálogo de Elementos

Nombre	Tipo	Descripción	Prop.
Active Directory Server	application-component	Los tipos de autenticación realizadas a partir de las identidades administradas de los recursos de Azure, entidades de Servicio y Certificados, podrán ser integrado con los dominios del directorio activo (DA) local. Por lo que respecta a la autenticación, será generado con la asignación de usuarios y credenciales definidas alineadas con la política Específica de Control de Acceso., a partir de la integración será validado el ingreso a las diferentes soluciones y/o sistemas de información de la PGN.	
App PGN Web	application-component		*plataforma:* angular 11 *brecha:* 100
Funcionarios Autorización	business-actor	Verificación que se realiza con la identidad del Servidor público, Contratista, Aprendiz y/o practicante de la entidad, proceso que se lleva a cabo cuando se ingresa al sistema, a la red o a cualquier base de datos. 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, que definirá la complejidad para la administración de contraseñas (Conjunto de caracteres variado con minúsculas, mayúsculas y números, entre otros).	

Seguridad.DesarrolloSeguro.

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

Metodología sobre el Desarrollo de Código Seguro..

versión 0.2

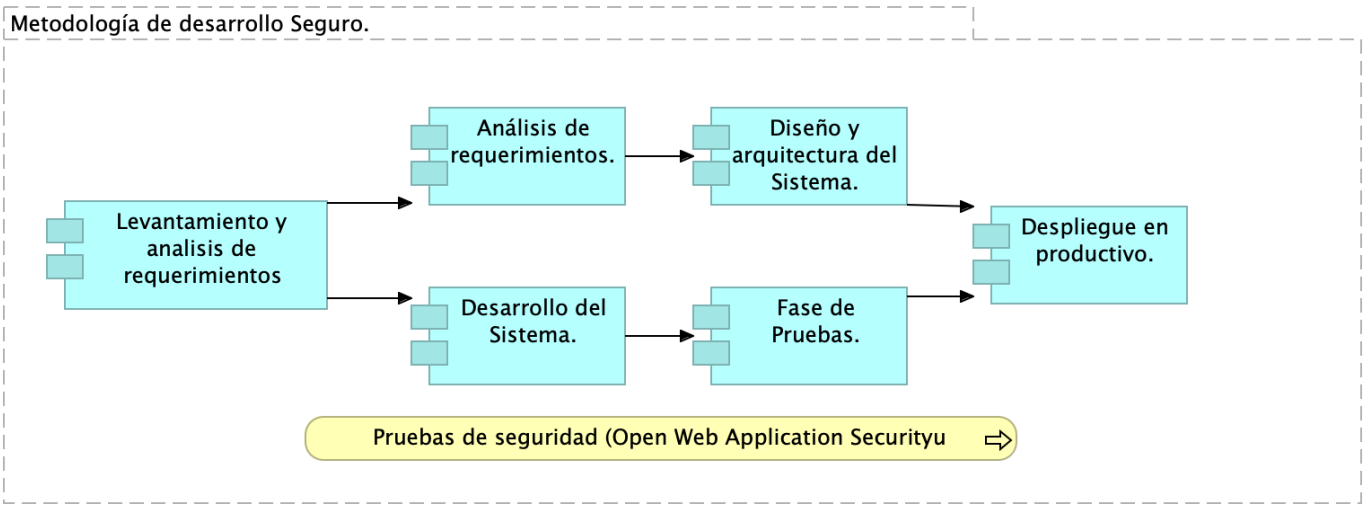


Imagen 15: Vista. Seguridad.DesarrolloSeguro.

METODOLOGÍA DE DESARROLLO.

La metodología de desarrollo seguro implementa las formas del desarrollo en cada una de las fases que se han requerido para los desarrollos de módulos misionales (SIM), Registro de Inhabilidades (SIRI), módulos de control interno, relatoría, entre otros, definido a partir de la metodología S-SDLC (Secure Software Development Life Cycle), que define los requisitos de seguridad a lo largo de las distintas fases de construcción del software: análisis de requerimientos, diseño y arquitectura del sistema, desarrollo del Sistema, Fase de pruebas y despliegue en productivo.

Migración de datos: Se presentarán los mecanismos adecuados para realizar la migración de la información que se encuentran en los sistemas de información desarrollados. Principios de seguridad. El siguiente contenido relaciona los lineamientos de seguridad definidos en The Owasp Foundation (Open Web Application Security Project) que deberían cumplirse para el desarrollo de las diferentes soluciones de software.

Principio de menor privilegio: La asignación de los permisos estará validados de tal forma que los Servidores Públicos, Contratistas, Practicantes y/o aprendices que interactúen con las diferentes soluciones dispongan mínimos privilegios necesarios para efectuar las actividades.

Defensa en profundidad: Es importante identificar diferentes factores de riesgos que permita encontrar fallas en las soluciones, Este análisis podrá ser obtenido como resultado de las pruebas de seguridad, y como resultado las remediaciones que se deben implementar para ejecutar los planes de acción y lograr reducir las vulnerabilidades. Segregación de permisos: Tener en cuenta que los permisos de acceso solo deben estar asignado a los responsables de los desarrollos con acceso con acceso a los diferentes ambientes. Seguridad en la ofuscación de datos. Como se ha venido planteando, los mecanismos para el ofuscamiento de los datos, a partir de los diferentes mecanismos de cifrados, como el TLS, SSL y HTTPS. Solucionar de manera correcta los problemas de seguridad: La identificación de un problema de seguridad, y la solución deberá plantearse a partir de pruebas que permitan verificar que la falla de seguridad ha sido solucionada. Estos resultados serán dados con los reportes de las prueba realizadas sobre las soluciones a través de la metodología del OWASP (Open Web Application Security Project). Codificación: Se mencionan los principales controles que se deben tener en cuenta para la realización de la codificación del software: • Capa de datos. • Gestión de Logs. • Controles de acceso. • Codificación de caracteres.

LINEAMIENTOS.

Tipo de sistema:

Los sistemas de información debe ser aplicaciones web, compatible con los navegadores que encabecen el mercado, actualmente: Chrome, Internet Explorer, Mozilla Firefox, o cualquier otro navegador. Deberá ser compatible con dispositivos móviles, por lo que el diseño deberá ser responsive Accesibilidad

Los sistemas web desarrollados deberán dar cumplimiento a los estándares de accesibilidad y usabilidad definidos por el Ministerio de las tecnologías de la Información y las comunicaciones MINTIC.

REPOSITORIO El repositorio del código fuente se encuentra en Azure DevOps, y para ser accedido deberá ser con la cuenta de correo corporativo.

Catálogo de Elementos

Nombre	Tipo	Descripción	Prop.

Nombre	Tipo	Descripción	Prop.
Análisis de requerimientos.	application-component	Se identifican los requerimientos funcionales y no funcionales que sirven como instrumento para el desarrollo de las soluciones. La etapa de análisis terminará con el entendimiento de los requerimientos y la priorización de estos. La identificación de los nuevos requerimientos que surjan por parte del cliente, serán revisado y validados para su posterior aprobación.	
Desarrollo del Sistema.	application-component	La presente fase del ciclo de vida, se da a partir de la construcción, adaptación e integración de la solución. El equipo de desarrollo implementará la solución, incorporando metodología ágil, con la planeación, ejecución de Sprint, con retroalimentación y retrospectivas cíclicas o iterativas hasta que finalice el desarrollo de la solución, se tendrá en cuenta el desarrollo de los códigos fuentes documentados y probados, bases de datos de las soluciones y la documentación técnica.	
Despliegue en productivo.	application-component	Se despliega en producción para iniciar el consumo por parte de los servidores públicos, contratistas, aprendices y/o practicantes de la Procuraduría General de la Nación. Se realizará el acompañamiento para el despliegue para garantizar el correcto funcionamiento de las soluciones desarrolladas, y las actividades de conocimientos con sus manuales establecidos.	
Diseño y arquitectura del Sistema.	application-component	El detalle de los componentes se generará a partir de la definición de la arquitectura de software que definirá los patrones y lineamientos para la construcción de las soluciones, que estarán definidos en el documento de arquitectura de Software y planteará la arquitectura de i) Software, ii) datos, iii) infraestructura y iv) modelo de Seguridad.	
Fase de Pruebas.	application-component	El desarrollo de la presente fase permitirá crear el ambiente adecuado para la ejecución de las pruebas, que permitirá registrar los resultados de las pruebas realizadas. Se realizan pruebas integrales y/o funcionales con el fin de determinar la correcta operación de las soluciones o si es necesario efectuar cambios sobre alguna inconsistencia presentada por algún error o problemas de ejecución en el sistema desarrollado. Pruebas de Sistemas: Se tendrán en cuenta la realización de pruebas que permitan validar el correcto funcionamiento de cada módulo de las soluciones, con el fin de verificar que cada módulo funciones de forma correcta. (rendimiento, concurrencia, Pruebas de carga y estrés). Pruebas de funcionalidad: Se realizarán las pruebas de herramientas para garantizar que las soluciones cumplen con los objetivos definidos y especificados, teniendo en consideración los diferentes escenarios de integración con otros aplicativos propios de la procuraduría general de la Nación. Pruebas de vulnerabilidad: Se realizarán las pruebas de seguridad y generación de informe que permitirá identificar las posibles vulnerabilidades del desarrollo de las soluciones propuestas.	
Levantamiento y analisis de requerimientos	application-component		
Pruebas de seguridad (Open Web Application Securityu Project)	business-process		
Metodología de desarrollo Seguro.	grouping		

Seguridad.LogsAuditoría.

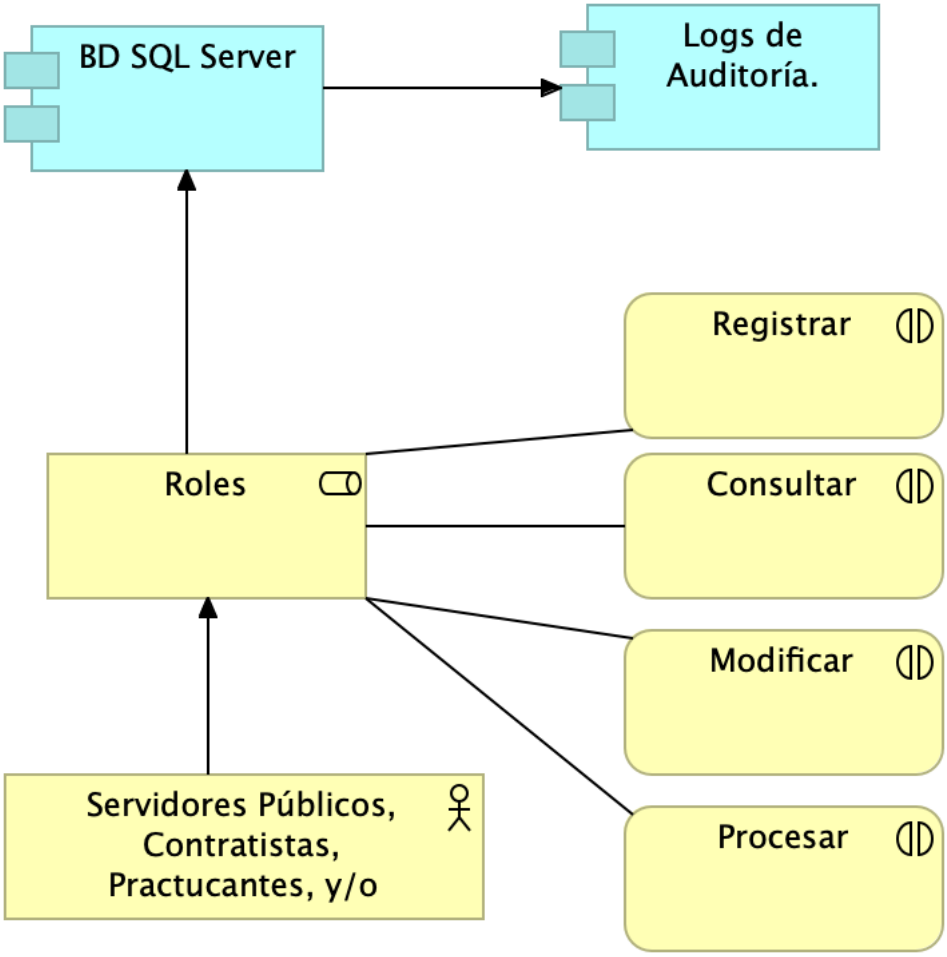


Imagen 16: Vista. Seguridad.LogsAuditoría.

Catálogo de Elementos

Nombre	Tipo	Descripción	Prop.
BD SQL Server	application-component	Los datos estarán procesados y almacenados en las bases de datos, el cual tendra implementados mecanismos de seguridad para el cifrado de los datos. Para el respaldo de las bases de datos en los ecosistemas de Dev, Test, Prod se cuenta con las siguientes políticas de retención de copias de seguridad y frecuencia de copias de seguridad definidas en el gestor de bases de datos. Para la base de datos de seguridad y configuración de la aplicación se tiene un plan de copia completo cada 12 horas (PITR) en una franja de tiempo de 35 días. Adicionalmente cuenta con un LTR de conservación de 12 semanas para las copias de seguridad semanales, 12 semanas de conservación para la primera copia de seguridad de cada mes, y una conservación de 12 semanas de una copia de seguridad anual. Para la base de datos de datos y trazabilidad de transacciones de la aplicación se tiene un plan de copia completo cada 12 horas (PITR) en una franja de tiempo de 35 días. Adicionalmente cuenta con un LTR de conservación de 52 semanas para copias de seguridad semanales, 52 semanas de conservación para la primera copia de seguridad de cada mes, y una conservación de 52 semanas de una copia de seguridad anual. Esto con la finalidad de que al ser una base de datos transaccional precisa de una conservación completa de los años transaccionales.	

Nombre	Tipo	Descripción	Prop.
Logs de Auditoría.	application-component	El histórico de transacciones queda registrado en cada tabla donde se guarda la información y una especial llamada HistoryLogs para el tema de auditoría. En los documentos definidos del proyecto se observa la estructura que presenta el log dando cumplimiento al requerimiento de seguridad frente al registro de eventos. Esto permite tener registro de la tabla afectada, los datos afectados, el registro afectado, el tipo de evento asociado a la transacción, la fecha de la transacción, la dirección IP del origen y el usuario quién realizó la misma. Del mismo modo, cada entidad dentro del sistema cuenta con los atributos relacionados en el json como complemente a la trazabilidad de la información. Se tendrán registros de los ingresos al sistema la aplicación y las actividades realizados por los usuarios.	
Servidores Públicos, Contratistas, Practucantes, y/o Aprendices.	business-actor		
Consultar	business-interaction	Permitirá identificar los Servidores públicos, Contratistas, Practicantes y/o aprendices que podran Consultar informacion sobre las diferentes soluciones.	
Modificar	business-interaction	Permitirá identificar los Servidores públicos, Contratistas, Practicantes y/o aprendices que tendrán acceso a modificar/ Actualizar informacion sobre las diferentes soluciones.	
Procesar	business-interaction	Permitirá identificar los Servidores públicos, Contratistas, Practicantes y/o aprendices que podran inactivar información sobre los diferentes sistemas de información.	
Registrar	business-interaction	Permitirá definir los Servidores públicos, Contratistas, Practicantes y/o aprendices que podran registrar informacion sobre las diferentes soluciones.	
Roles	business-role		

Seguridad.Owasp

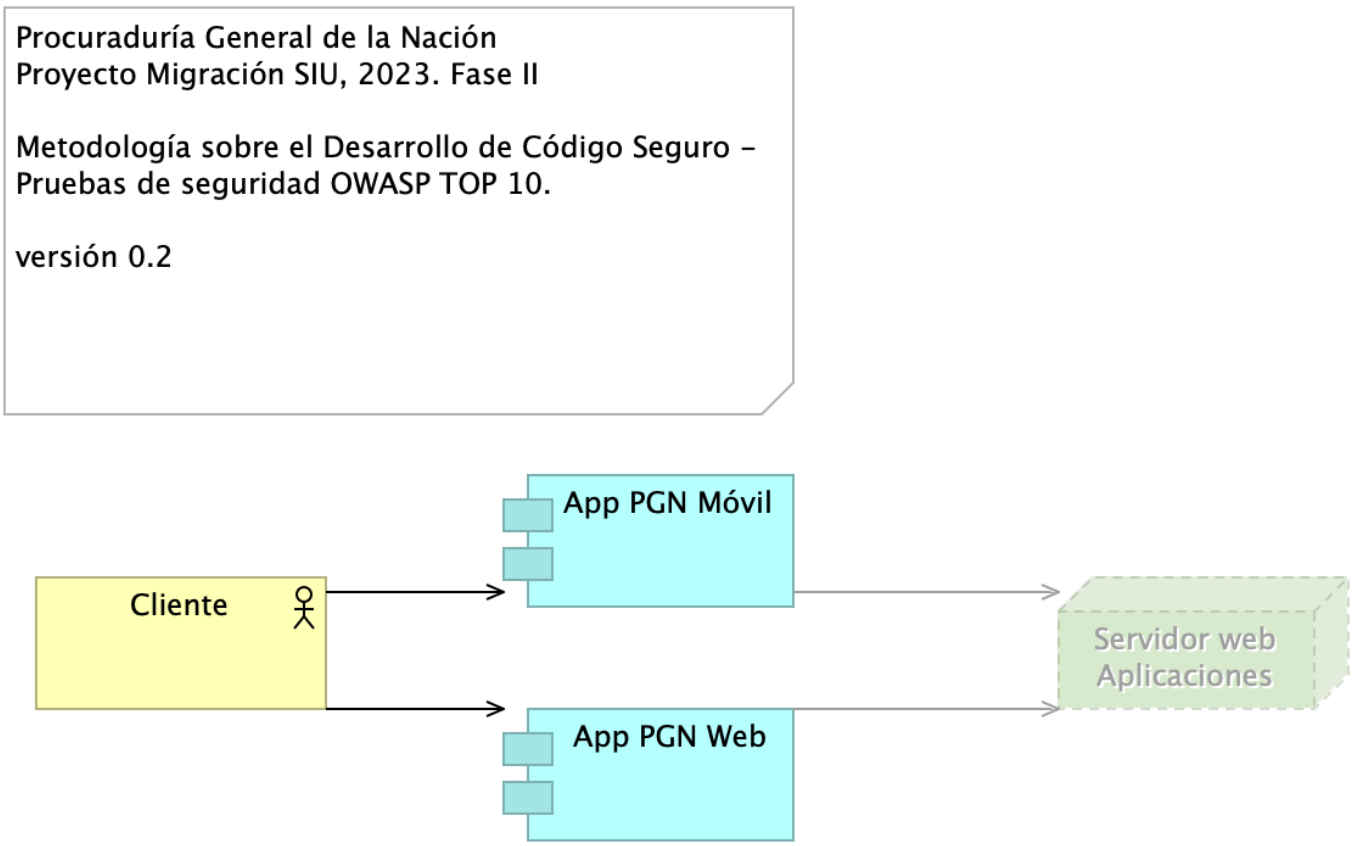


Imagen 17: Vista. Seguridad.Owasp

Durante todo el proceso se realizarán pruebas de ánalisis de vulnerabilidades que pueda tener el sistema. Se establecerán puntos donde el software esté preparado para dicho análisis. En conjunto con el lider de Seguridad, se analizarán las posibles vulnerabilidades y se revisarán cuales pueden ser mitigadas y cuales pueden ser omitidas. Para el paso a producción, se realizará un ultimo análisis de vulerabilidades y se tendrá en cuenta la revisión de las acciones de mitigación, con el fin que se hayan resuelto.

La empresa establecerá buenas prácticas para el desarrollo seguro de software, a partir de la implementación del estandar internacional OWASP (Open Web Application Security Project). El proposito principal será garantizar la seguridad de las soluciones de la Procuraduría General de la Nación PGN. Se tiene en cuenta lineamientos técnicos de acuerdo con las normas establecidas en top ten (10) del OWASP:

Código de Injección SQL: Vulnerabilidad que se puede presentar por intermedio de peticiones o consultas a las bases de datos, y las entradas de la aplicación no son controladas debidamente.

Controles: - Descarte de caracteres especiales, espacios que innecesarios del lado del cliente y/o servidor. - Verificación de caracteres incluidos en consultas SQL o LDAP, para el lado cliente como servidor. - Limitación cantidad de caracteres del campo creado. - Verificación del resultado de consulta, que genere resultado de consulta o ningun resultado (Si es mostrado mas de un resultado, deberá ser considerado error). - Numero de intentos fallidos por ingreso de contraseñas.

Falla en las autenticación y Administración de Sesión: Presentada debido a las fallas en la administración de las funciones de autenticación o sesión. (Como exposición de usuarios, contraseñas e identificador unico).

Controles: - Descarte por caracteres especiales. espaciones que innecesario como para el lado del servidor y cliente. - Verificacion de meta caracteres SQL o LDAP, para el lado del servidor y cliente. - Validar el uso del método POST, si se envían datos de servidores publicos y/o contratistas. - No permitir el almacenamiento de datos de los funcionarios en las cookies. - Limitación de los tiempos en las sesiones.

Técnicas de Cross Site Scripting XSS: Vulnebilidad presentada cuando los datos de entrada son utilizados para desarrollar el contenido del sistema de información, sin validar la informción que se envía ppor la URL.

Controles: - Revisar la incorporación de caracteres especiales, espacios que no sean necesarios dentro del campo de texto, asi como para el lado del cliente y el servidor.

Referencias directas a objetos de forma insegura: Presentada cuando se referencia a un objeto interno, tal como directorio, archivo, algun registro de la base de datos BD en la URL, y no establecen los respectivos controles para el acceso a los recursos.

Controles: - Evitar el uso de campo de referencia, podrá ser modificado con facilidad. - Verificación de objeto válido en el envío de datos. - Identificar los tipos de datos y objetos a enviar y los métodos de uso para cada uno de estos.

Cross site Request Forgery (CSFR): Presentado en aplicaciones donde las peticiones son faciles de predecir a partir del uso de comandos que son transmitidos por un usuario desconocido.

Controles: - Evitar variables en las URL, si es posible utilizarlas, se deberá comprobar la información que contiene. - Tener en cuenta el envio de información que se envía por las URL. - Tener en cuenta el uso de token como herramienta de validación. - Validacion de sesiones.

Pobre Mala Configuración de Seguridad: Puedo presentarse cuando se dejan las cuentas de accesos por defecto, archivos y directorios si establecer controles de seguridad, generando puertas traseras que pueden ser aprovechadas por los ciberdelincuentes para vulnerar el sistema de información. Controles: - Asignar nuevas configuraciones a las definidas de fabrica. - El personal de infraestrutura debera tener en cuenta los requerimientos de la aplicacion para establecer las configuraciones adecuadas. - Se debe tener en cuenta la habilitación de los servicios estrictamente necesarios.

Almacenamiento inseguro de Criptografía: Se presenta por debilidades en el proceso de implementación de controles criptograficos, algoritmos de cifrado y almacenamiento inseguro de llaves.

Controles: - Algoritmos de cifrado (AES, SHA-256). - Para el uso de controles asimetricos, tener en cuenta la custodia de las llaves privadas. - Seguridad en la capa de transporte TLS y certificados SSL. - Cifrado de datos sensibles.

Falla al restringir acceso por URL: Se presenta cuando se generan solicitudes a las paginas y no se encuentran protegidas adecuadamennte. Son modificadas las URL para obtener el acceso con privilegios.

Controles: - La cuenta de algun servidor público con menor privilegio de acceso a la solución, modificar la URL para verificar el acceso, si es aceptado el acceso, se identifica que el sistema de información es vulnerable.

Redirrecionamiento y reenvíos sin validación: Con frecuencia las aplicaciones envian hacia otras páginas cuando se ejecutan parametros que no son validados, el atacante puede definir el sitio al que se quiere redireccionar.

Controles: - Validación del campo de referencia, analizador de registros web, para proteger de ataques XSS y otros tipos de ataques. - Verificación de privilegios.

Insuficiente protección de la capa de transporte: Se presenta si la informacion que viaja por internet no se encuentra debidamente protegida. Un usuario externo que monitoree la red, podrá obtener información (Usuarios, Contraseñas e Identificación). Controles: - Vulnerabilidad enfocada a nivel de infraestructura. Podrá ser utilizado un Snnifer para el monitoreo de la red.

Los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la “Guía de desarrollo OWASP” y “OWAS Cheat Sheet, permitirá realizar pruebas de seguridad integrando el analisis de vulnerabilidades, y pruebas de Ethical Hacking. Los resultados permitirán identificar los requisitos de seguridad que los sistemas de informacion o servicios web deberán cumplir. La metodologia empleada tendrá las siguientes fases:

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

• ANÁLSIS DE VULNERABILIDADES: Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades.

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

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

No URL IP 1. https://runtimetest.lappiz.io/#/auth/login/PGN_Lappiz 135.181.185.207

El Login deberá evidenciar el control de errores, al momento de realizar la validación deberá mensaje de error para el caso que se autentique con credenciales erradas.

Catálogo de Elementos

Nombre	Tipo	Descripción	Prop.
App PGN Móvil	application-component		
App PGN Web	application-component		
Cliente	business-actor		
Servidor web Aplicaciones	node		

`Generated on: Thu Nov 09 2023 09:20:37 GMT-0500 (COT)`

Requerimientos de Administración

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

6. Las soluciones deben permitir la configuración de permisos de consulta con diferentes alcances para cada tipo de usuario.
7. Desde la interfaz de usuario se debe poder crear, modificar o inactivar usuarios, perfiles o roles, permisos a las diferentes funcionalidades de la solución.
8. Las soluciones deben permitir la definición de varios tipos de usuario.
9. Las soluciones deben permitir la parametrización de los consecutivos que maneja la entidad para los diferentes documentos generados por las soluciones.
10. Debe permitir parametrizar la vinculación del consecutivo a un documento en forma manual o automática.
11. Las soluciones deben permitir que se configure la autenticación de forma interna integrándose con LDAP el acceso de los usuarios y actores de las diferentes dependencias de la entidad que interactúen con los demás sistemas.

Requerimientos de Seguridad

1. Las soluciones deben dar cumplimiento a las políticas institucionales del sistema de gestión de seguridad de la información establecidas por la entidad que busca garantizar la confidencialidad, integridad y disponibilidad de la información que se genera, procesa, almacena y/o transmite en los sistemas de Información de la Entidad.
2. Las soluciones de automatización de procesos a implementar deben permitir la Gestión de Seguridad de Usuarios, grupos de usuarios y asignación de Roles y perfiles de usuarios, permitiendo asociar las acciones disponibles en la solución con respecto a roles de usuario, permitiendo parametrizar las funcionalidades que cada actor puede usar en la solución.
3. Un usuario puede estar asociado a uno o más roles, de tal manera que los menús de navegación de la solución se muestran o despliegan dependiendo de las acciones asociadas a cada rol de usuario, permitiendo así que cuando el usuario es autenticado correctamente, la solución verifica los roles que tiene activos para otorgarle únicamente las acciones autorizadas.
4. El diseño de la solución debe definir los criterios necesarios para asegurar la trazabilidad y auditoría sobre las acciones de creación, actualización, modificación o borrado de los componentes de información, de tal manera que la solución debe permitirle al administrador de la solución parametrizar las tablas y eventos que pueden auditarse.
5. Las soluciones deben tener en cuenta mecanismos que aseguren el registro histórico para poder mantener la trazabilidad de las acciones realizadas por los usuarios, contemplando el registro de auditoría que contiene información de fecha y hora, identificación del registro, tabla afectada, descripción del evento, tipo de evento, usuario que realiza la acción, identificación de sesión y dirección IP del usuario que efectuó la transacción.
6. La solución debe proveer una consulta que permita a un usuario con los privilegios asignados, consultar los registros de auditoría, aplicando criterios de filtro (usuario, maquina, rango de fechas y tipo de operación).
7. Las soluciones deben integrarse con LDAP – (Lightweight Directory Access Protocol) para los procesos de inicio de sesión y autenticación. La solución debe soportar la integración Nativa con Active Directory de Microsoft. Para usuarios externos el mecanismo de autorización, autenticación y acceso será controlado a través del modelo de seguridad de la solución (no habrá autenticación para usuarios externos).
8. Las soluciones deben cumplir con los lineamientos de seguridad relacionados a su utilización a través de redes públicas y privadas, garantizando la confidencialidad e integridad de la información y acceso a ella.
9. Debe evidenciar que, a través de pruebas de vulnerabilidad, garantiza la seguridad de la información. Estas pruebas deben suministrar evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad.
10. Debe incluir un mecanismo de cifrado de los datos que se transportan entre los diferentes componentes tecnológicos y los datos sensibles de la base de datos que representen un alto nivel de confidencialidad.
11. A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio).
12. Debe contemplar el cumplimiento de la normatividad vigente en cuanto a protección de datos personales y debe permitir el manejo de excepciones.
13. Para los casos que aplique se debe permitir el manejo de certificados y/o firmas digitales en los documentos que así se definan para efectos de aprobación y digitalización.
14. Debe contemplar las prácticas de desarrollo seguro de aplicaciones y/o implementación segura de productos, para su naturaleza Web based.
15. Debe funcionar sobre protocolo SSL (certificados internos de la entidad cuando los sistemas de información sean internas y certificados validos públicamente cuando los sistemas de información estén expuestas a internet).
16. Debe entregar un procedimiento para el respaldo de la información de acuerdo con las necesidades de la entidad.
17. Debe incluir uso de criptografía para transacciones y/o campos sensibles según lo indiquen las normas vigentes y las necesidades específicas del negocio de acuerdo como lo determine la entidad.
18. Debe contemplar un modelo de datos que garantice base de datos única para evitar que se pueda presentar duplicidad de información.
19. En la información confidencial solo puede ser consultada por los perfiles autorizados e igualmente restringir documentos de consulta según los privilegios o permisos asociados.
20. A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio).
21. Debe cerrar las transacciones luego de máximo 10 minutos de inactividad.
22. Debe incluir controles de bloqueo de cuenta después de un máximo de 5 intentos erróneos a fin de evitar ataques de fuerza bruta.
23. Debe evidenciar el resultado positivo frente apruebas de ethical hacking, análisis de vulnerabilidades, carga, estrés y desempeño antes de la puesta en operación de acuerdo con los lineamientos de la entidad.
24. Debe cumplir con todos los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la “Guía de desarrollo OWASP” y “OWAS Cheat Sheet”.

Anexos

Modelo ER del SIU Migrado

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

Referencias

[1] [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/