

Documento de Arquitectura Migración Funcional PGN SUI

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

Versión del producto 1.6423462 de 05 Dec 2023

Presentado a

Procuraduría General de la Nación (PGN)

Fecha

05 Dec 2023

Los productos de esta etapa, Migración Funcional SUI, Contrato 078-2023, ([Web](#)) están basados en el resultado de la Fase 1 del proyecto PGN SUI del 2022, Sharepoint.Softgic@6423462 del December 5, 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 SUI 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 SUI
Palabras clave	SUI, Softgic, PGN, Análisis de brecha, GAP, Comparativa
Autor	
Fuente	
Versión	
1.6423462	2023-12-05. pptx-pgn
1.30bf403	2023-12-05. pptx-pgn
1.20c257e	2023-11-29. doc SUI*
1.af72748	2023-11-29. doc SUI*
1.a95d7c9	2023-11-28. doc-nov
1.ce7fa4e	2023-11-28. doc-nov
1.61ab07e	2023-11-28. doc-nov
1.2774000	2023-11-23. arqdoc1
1.3996a6d	2023-11-23. arqdoc1
1.bd9674d	2023-11-23. ppt1
Vínculos	N003a Vista Segmento PGN SUI

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 SUI, están determinados por el uso de las plataformas específicas determinadas por la implementación (desarrollo del software).
4. Requerimientos de interoperabilidad. Los recursos de interoperabilidad y colaboración entre sistemas, módulos, submódulos y aplicaciones de terceros relacionados con esta Fase del proyecto son los mismos a tener en cuenta en los diseños de la solución de esta Fase 2. Otros recursos a considerar son los descritos en el anexo técnico del contrato del proyecto.
5. Requerimientos de protocolos o interfaces. Los recursos de red, y protocolos de comunicación o transporte de esta Fase del proyecto a tener en cuenta en los diseños de la solución de esta Fase 2 parten de la base de los considerados en la anterior Fase 1. Otros recursos a considerar son los descritos en el anexo técnico del contrato del proyecto.
6. Seguridad. Las restricciones de seguridad del proyecto actual a tener en cuenta en los diseños de la solución de esta Fase 2 parten de la base de las de la anterior Fase 1. Esto es, los que están descritos en el anexo técnico del contrato del proyecto.

Restricciones Secundarias

Otras restricciones a detallar.

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

Requisitos de Arquitectura (no funcional)

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

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

Requerimientos generales

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

Requisitos de Arquitectura (no funcional) Particulares

Extensibilidad SUI

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

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

Mantenibilidad SUI

Tabla 2: Requisito no. 2.

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

Arquitectura de Información (Datos)

- [Diagrama Modelo de Datos Conceptual](#)
 - [Migracion.2a.a1.Datos Información](#)
- [Diagrama Modelo de Datos Físico \(diagramas entidad-relación\)](#)
 - [Migracion.2a.a3. Datos Modelo Físico](#)
- [Diagrama Modelo de Datos Lógico](#)
 - [Migracion.2c1. Datos SIM](#)
 - [Migracion.2c. Datos Hominis](#)
 - [Migracion.2c3. Datos Control Interno](#)
 - [Migracion.2c2. Datos SIRI](#)
- [Documento Diccionarios de Datos](#)
 - [Migracion.2a.a2. Datos Diccionario](#)
- [Mapa de Información \(flujos de información\)](#)
 - [Migracion.2d2. Datos Organización](#)
 - [Migracion.2d3. Datos Transporte \(flujo SUI - SIM\)](#)
 - [Migracion.2d4. Datos Transporte \(flujo SUI - SUI\)](#)
- [Modelo Ontológico](#)
 - [Migracion.2a.a34 Datos Ontológico](#)

Diagrama Modelo de Datos Conceptual

Migracion.2a.a1.Datos Información

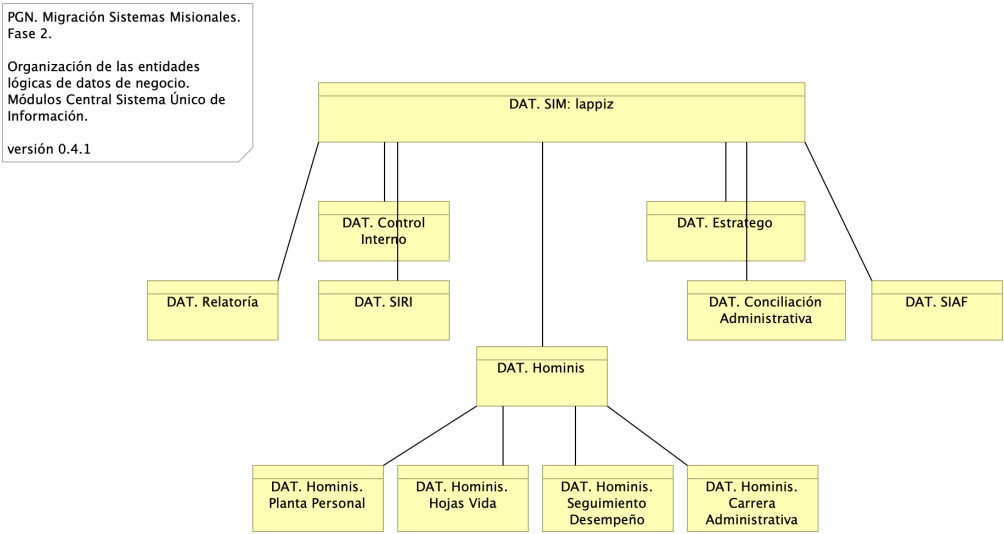


Imagen 1: Vista. Migracion.2a.a1.Datos Información

Modelo de información. Organización y jerarquía de los grupos de datos (dominios) del SUI Migrado, 2023.

Dominios Principales de Información SUI Migrado

- Dominio común: SIM
- Dominios individuales
 - Hominis: Planta de personal, Hojas de vida, Seguimiento de desempeño, Carrera administrativa
 - Conjunto de datos Relatoría
 - Control Interno
 - Conciliación Administrativa

Catálogo de Elementos

Nombre	Tipo	Descripción	Prop.
DAT. Conciliación Administrativa	business-object	Entidades de datos de negocio de capital humano de la PGN. Sistema de información Homini.	
DAT. Control Interno	business-object		
DAT. Estrategico	business-object	Entidades de datos de negocio de capital humano de la PGN. Sistema de información Homini.	

Nombre	Tipo	Descripción	Prop.
DAT. Hominis	business-object	Entidades de datos de negocio de capital humano de la PGN. Sistema de información Homini.	
DAT. Hominis. Carrera Administrativa	business-object	Entidades de datos de negocio de capital humano de la PGN. Sistema de información Homini.	
DAT. Hominis. Hojas Vida	business-object	Entidades de datos de negocio de capital humano de la PGN. Sistema de información Homini.	
DAT. Hominis. Planta Personal	business-object	Entidades de datos de negocio de capital humano de la PGN. Sistema de información Homini.	
DAT. Hominis. Seguimiento Desempeño	business-object	Entidades de datos de negocio de capital humano de la PGN. Sistema de información Homini.	
DAT. Relatoría	business-object	Entidades de datos de negocio de capital humano de la PGN. Sistema de información Homini.	
DAT. SIAF	business-object	Entidades de datos de negocio de capital humano de la PGN. Sistema de información Homini.	
DAT. SIM: lappiz	business-object		
DAT. SIRI	business-object		

Diagrama Modelo de Datos Físico (diagramas entidad-relación)

Migracion.2a.a3. Datos Modelo Físico

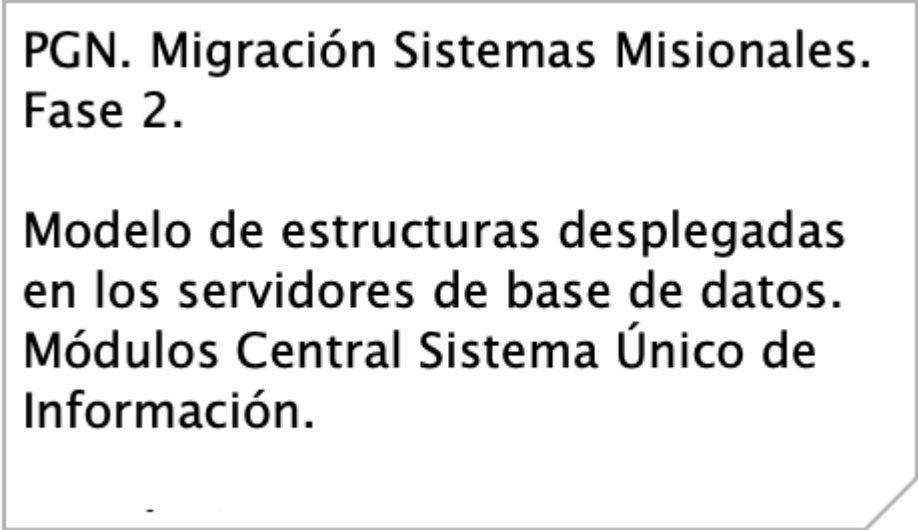


Imagen 2: Vista. Migracion.2a.a3. Datos Modelo Físico

Los modelos físicos representados en diagramas entidad - relación (ER) de los módulos SUI Migrado, como Hominis, Control Interno, Relatoría, SIRI, serán entregados como documentos aparte, anexos al documento actual en formato reproducible.

El formato reproducible en el que entregamos el modelo físico mediante la herramienta libre Draw.io.

Imagen 3: Vista. Migracion.2a.a3. Datos Modelo Físico

Imagen 3: Vista. Migracion.2a.a3. Datos Modelo Físico

Catálogo de Elementos

Nombre	Tipo	Descripción	Prop.
--------	------	-------------	-------

Diagrama Modelo de Datos Lógico

Migracion.2c1. Datos SIM

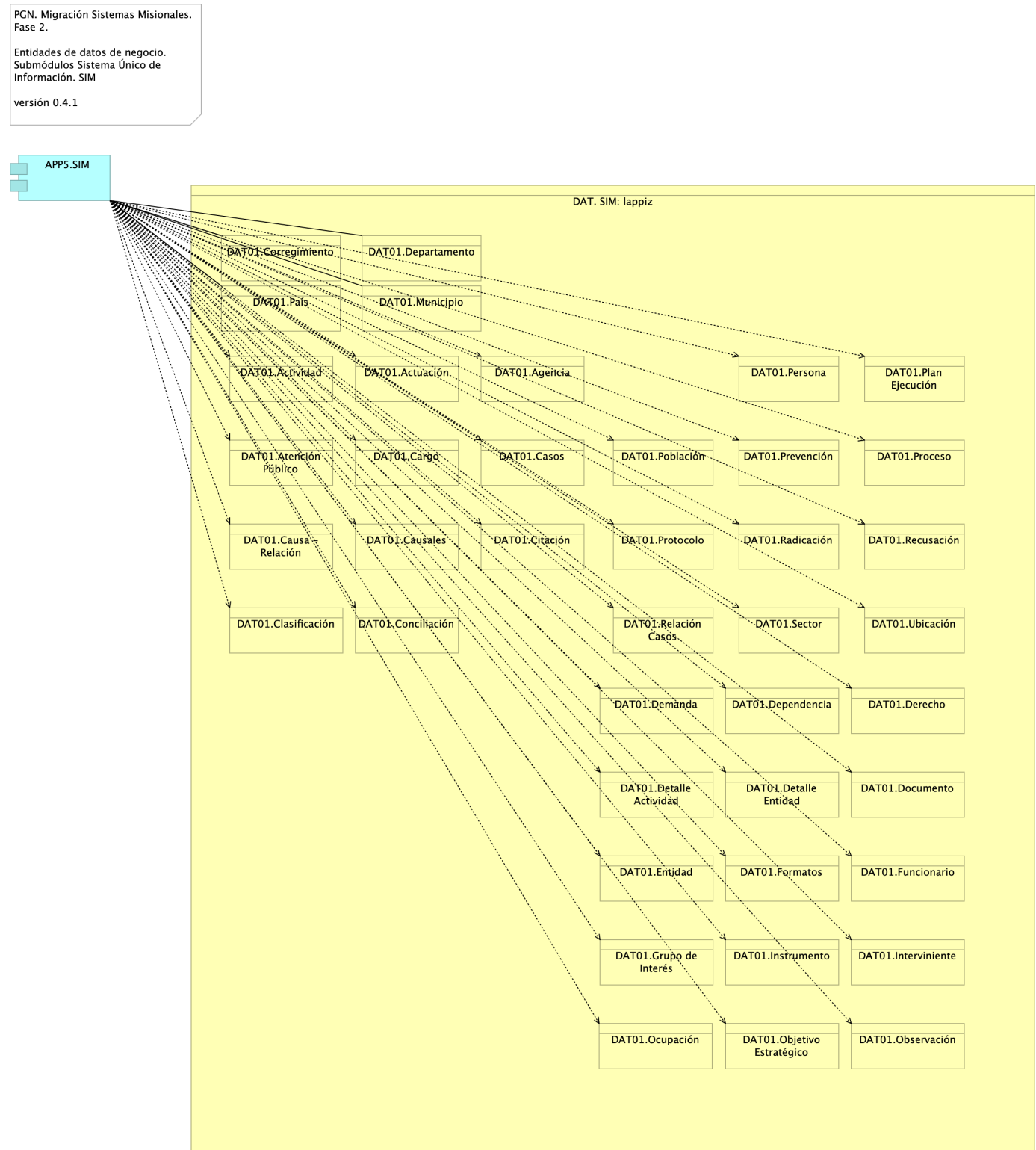


Imagen 4: Vista. Migracion.2c1. Datos SIM

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

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

Catálogo de Elementos

Nombre	Tipo	Descripción	Prop.
APP5.SIM	application-component	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN: SIM.	
DAT. SIM: lappiz	business-object		
DAT01.Actividad	business-object	Actividad del SIM	
DAT01.Actuación	business-object	Actuación del SIM	
DAT01.Agencia	business-object	Agencia del SIM	
DAT01.Atención Público	business-object		
DAT01.Cargo	business-object	Cargo del SIM	
DAT01.Casos	business-object	Casos del SIM	
DAT01.Causa - Relación	business-object		
DAT01.Causales	business-object	Causales del SIM	
DAT01.Citación	business-object	Citación del SIM	
DAT01.Clasificación	business-object	Clasificación del SIM	
DAT01.Conciliación	business-object	Conciliación del SIM	
DAT01.Corregimiento	business-object		
DAT01.Demanda	business-object	Demanda del SIM	
DAT01.Departamento	business-object	Departamentos del SIM.	
DAT01.Dependencia	business-object	Dependencia del SIM	
DAT01.Derecho	business-object	Derecho del SIM	
DAT01.Detalle Actividad	business-object		
DAT01.Detalle Entidad	business-object		
DAT01.Documento	business-object	Documento del SIM	
DAT01.Entidad	business-object	Entidad del SIM	
DAT01.Formatos	business-object	Formatos del SIM	
DAT01.Funcionario	business-object	Funcionario del SIM	
DAT01.Grupo de Interés	business-object		
DAT01.Instrumento	business-object	Instrumento del SIM	
DAT01.Interviniente	business-object	Interviniente del SIM	
DAT01.Municipio	business-object	Municipio del SIM	
DAT01.Objetivo Estratégico	business-object		
DAT01.Observación	business-object	Observación del SIM	
DAT01.Ocupación	business-object	Ocupación del SIM	
DAT01.País	business-object	País del SIM	

Nombre	Tipo	Descripción	Prop.
DAT01.Persona	business-object	Personas del SIM.	
DAT01.Plan Ejecución	business-object	Plan Ejecución del SIM	
DAT01.Población	business-object	Población del SIM	
DAT01.Prevencción	business-object	Prevención del SIM	
DAT01.Proceso	business-object	Proceso del SIM	
DAT01.Protocolo	business-object	Protocolo del SIM	
DAT01.Radicación	business-object	Radicación del SIM	
DAT01.Recusación	business-object	Recusación del SIM	
DAT01.Relación Casos	business-object	Relación casos del SIM	
DAT01.Sector	business-object	Sector del SIM	
DAT01.Ubicación	business-object	Ubicación del SIM	

Migracion.2c. Datos Hominis

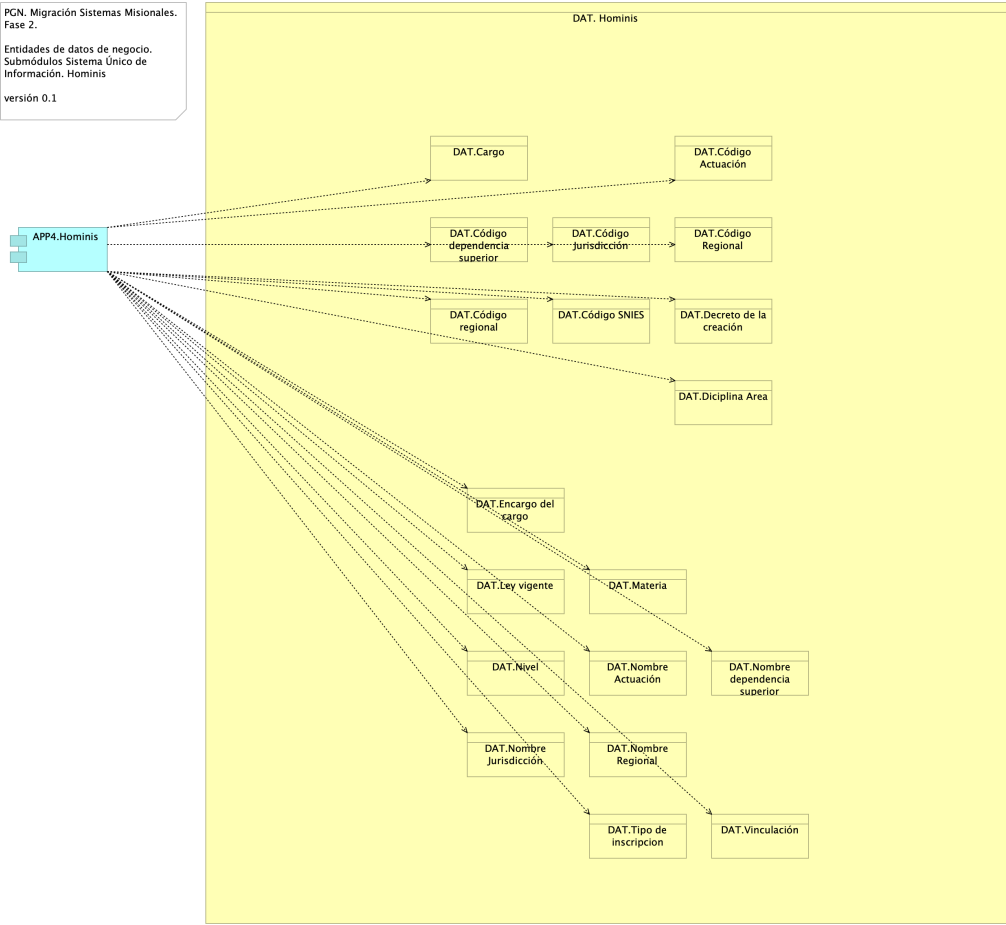


Imagen 5: Vista. Migracion.2c. Datos Hominis

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

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

Catálogo de Elementos

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

Migracion.2c3. Datos Control Interno

PGN. Migración Sistemas Misionales.
Fase 2.

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

versión 0.1

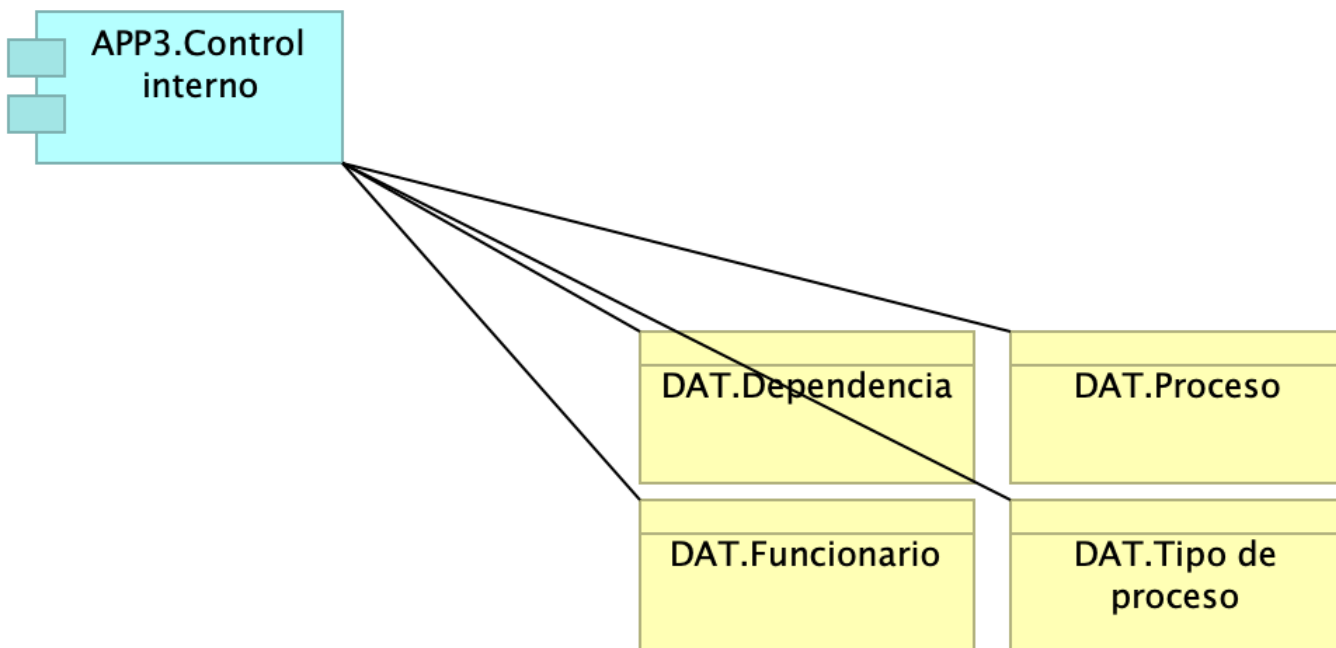


Imagen 6: Vista. Migracion.2c3. Datos Control Interno

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

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

Catálogo de Elementos

Nombre	Tipo	Descripción	Prop.
APP3.Control interno	application-component	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN: Control Interno.	
DAT.Dependencia	business-object		
DAT.Funcionario	business-object		
DAT.Proceso	business-object		
DAT.Tipo de proceso	business-object		

Migracion.2c2. Datos SIRI

PGN. Migración Sistemas Misionales.
Fase 2.

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

versión 0.1

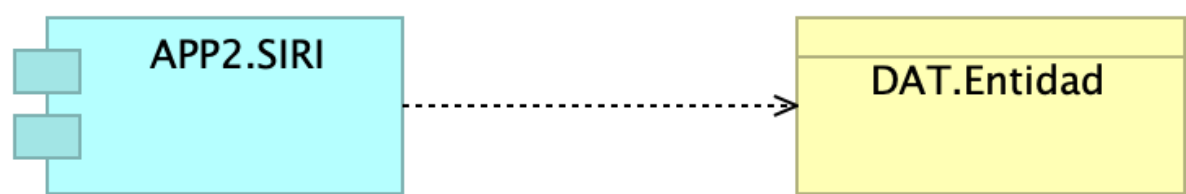


Imagen 7: Vista. Migracion.2c2. Datos SIRI

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

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

Catálogo de Elementos

Nombre	Tipo	Descripción	Prop.
APP2.SIRI	application-component	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN: SIRI.	
DAT.Entidad	business-object		

Documento Diccionarios de Datos

Migracion.2a.a2. Datos Diccionario

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

**Descripción de las entidades físicas
(diccionario). Módulos Central
Sistema Único de Información.**

versión 0.1

Imagen 8: Vista. Migracion.2a.a2. Datos Diccionario

Los diccionarios de datos explicativos de los modelos de datos físicos de los módulos del SUI Migrado, representados en tablas campo-descripción, serán entregados como documentos anexos aparte del documento de arquitectura de datos actual, y en formato reproducible.

El formato reproducible en el que entregamos los diccionarios de datos del modelo físico es DOCX.

Table PGN_Lappiz_ActividadPreventiva






Idx	Field Name	Data Type	Description
* 	Id	uniqueidentifier DEFAULT newid()	
	CEObservaciones	varchar(200)	
	Created_date	datetime	
	Edited_date	datetime	
	Created_by	uniqueidentifier	
	Edited_by	uniqueidentifier	
	RowStatus	varchar(1000)	
*	NombreActividad	varchar(500)	
* 	ActividadFK	uniqueidentifier	
*	CodigoNomActPreventiva	decimal() AUTOINCREMENT	
	UserEmail	varchar(100)	
	IpAddress	varchar(100)	
	EventType	varchar(100)	
Indexes			
	PGN_Lappiz_ActividadPreventiva_PK	ON Id	
Foreign Keys			
	PGN_Lappiz_ActividadPreventivaPGN_Lappiz_Actividad_ActividadFK_FK	(ActividadFK) ref PGN_Lappiz_Actividad (Id)	

Table PGN_Lappiz_AgenciaEspecial



Idx	Field Name	Data Type	Description
* 	Id	uniqueidentifier DEFAULT newid()	
	CEOrigenAgencia	varchar(200)	

Imagen 9: Migracion.2a.a2. Datos Diccionario

Catálogo de Elementos

Nombre	Tipo	Descripción	Prop.
--------	------	-------------	-------

Mapa de Información (flujos de información)

Migracion.2d2. Datos Organización

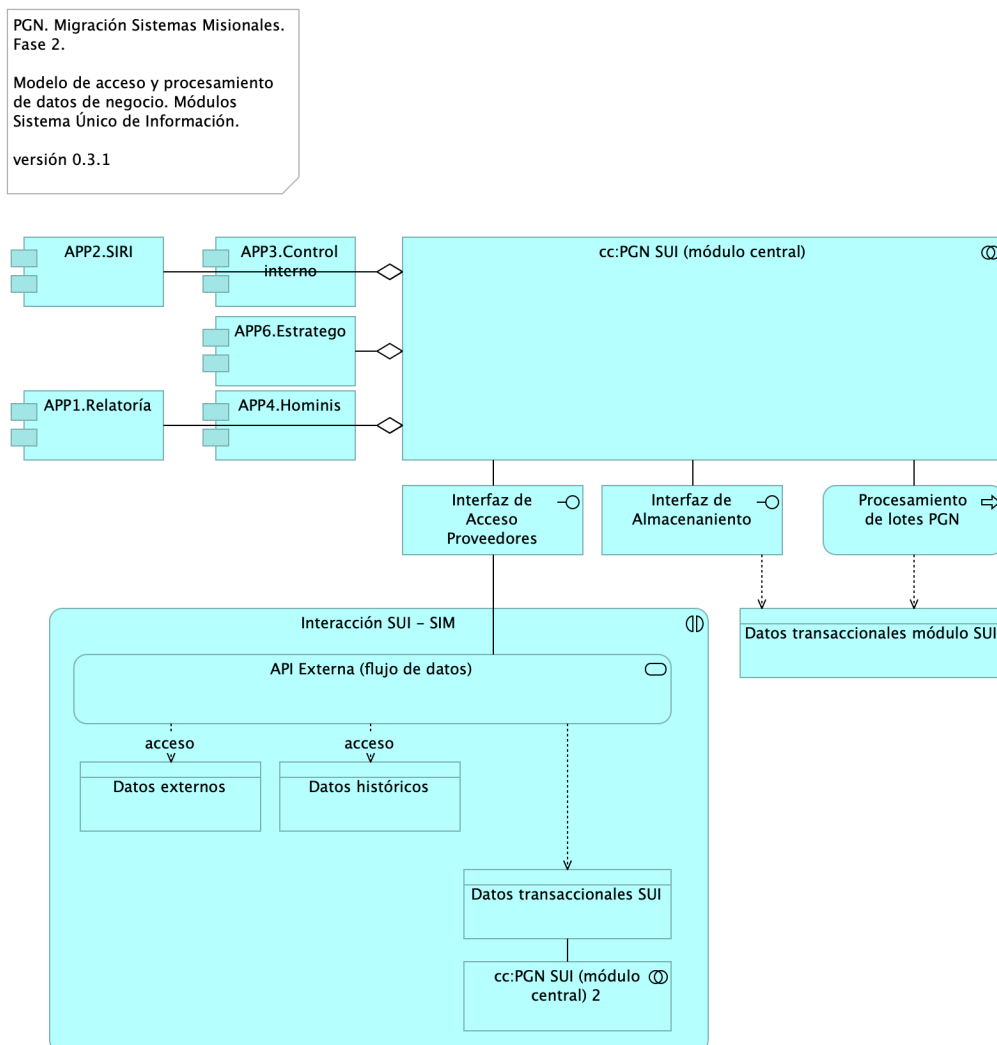


Imagen 10: Vista. Migracion.2d2. Datos Organización

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

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

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

Catálogo de Elementos

Nombre	Tipo	Descripción	Prop.
--------	------	-------------	-------

Nombre	Tipo	Descripción	Prop.
cc:PGN SUI (módulo central)	application-collaboration	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN.	
cc:PGN SUI (módulo central) 2	application-collaboration	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN.	
APP1.Relatoría	application-component	Módulo del SUI. Relatoría pública. Publicación de información de referencia para funcionarios y personas naturales, cientes de la PGN.	
APP2.SIRI	application-component	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN: SIRI.	
APP3.Control interno	application-component	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN: Control Interno.	
APP4.Hominis	application-component	Módulo del SUI. Gestión de capital humano, funcionarios y cargos de representación y libre remoción de la PGN.	
APP6.Estratego	application-component	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN: Estratego.	
Interacción SUI - SIM	application-interaction	Interacción de API SUI con API SIM para el transporte de entidades de negocio. Los tipos de datos que utilizan esta interacción entre aplicaciones son los datos externos al módulo central SUI que los requiera, los datos históricos que están por fuera del móduo SUI migrado, y los datos transaccionales de otros módulos SUI migrados.	

Nombre	Tipo	Descripción	Prop.
Interfaz de Acceso Proveedores	application-interface	Interfaz de acceso a los tipos de datos externos al SUI. El patrón de API Externa (reverse proxie) tiene el rol de unir y referir a los datos externos e históricos al SUI Migrado de tal manera que hace transparente la localización y el formato de este tipo de datos.	
Interfaz de Almacenamiento	application-interface	Interfaz de acceso a los repositorio, base de datos relacionales y no jerárquicas. Tipos de datos transaccionales, internos, del SUI.	
Procesamiento de lotes PGN	application-process	Los procesos de lotes, que requieren volúmenes de datos altos, deben hacer parte de la arquitectura de datos del SUI.	
API Externa (flujo de datos)	application-service	El patrón de API Externa (reverse proxie) tiene el rol de unir y referir a los datos externos e históricos al SUI Migrado de tal manera que hace transparente la localización y el formato de este tipo de datos.	
Datos externos	data-object		
Datos históricos	data-object		
Datos transaccionales SUI	data-object		
Datos transaccionales módulo SUI	data-object	Registros de trabajo de un módulo SUI Migrado, 2023.	

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

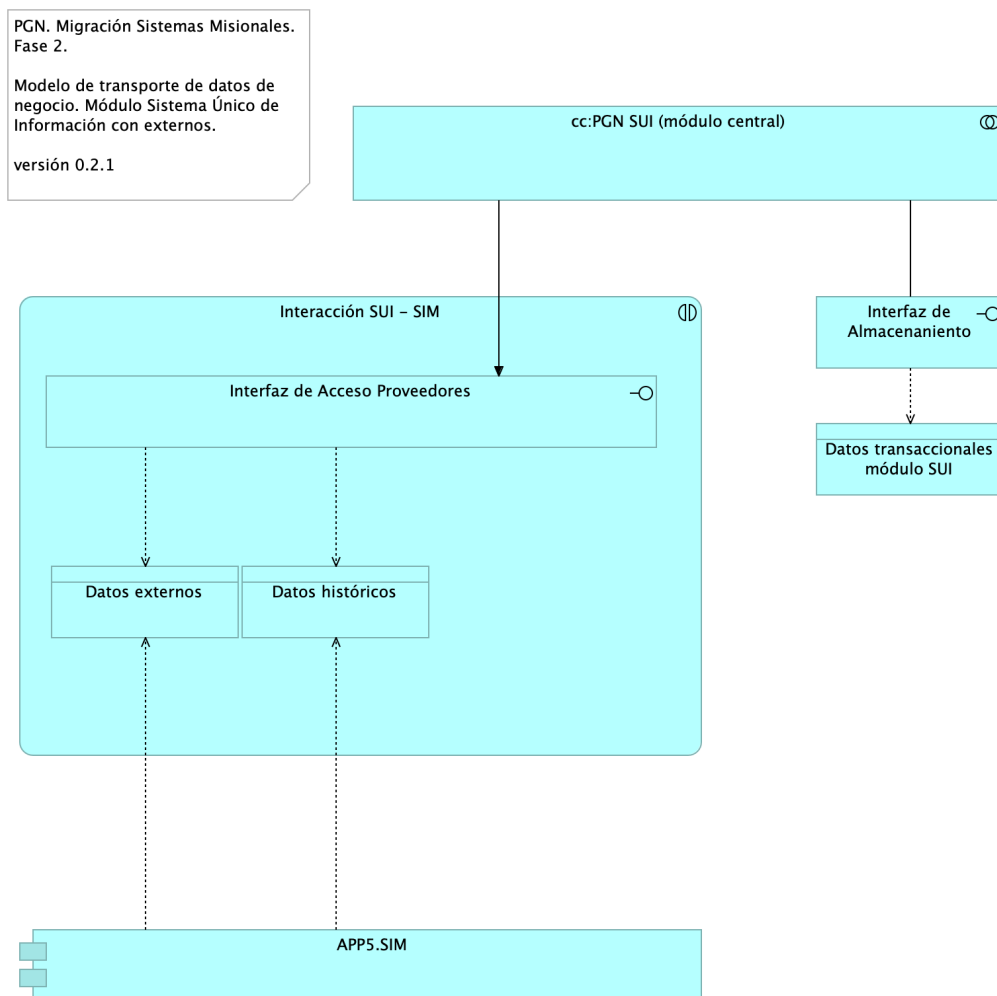


Imagen 11: Vista. Migracion.2d3. Datos Transporte (flujo SUI - SIM)

Modelo de acceso a datos de negocio del SIM.

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

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

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

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 particular de la PGN.	

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

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

PGN. Migración Sistemas Misionales.
Fase 2.

Modelo de transporte de datos de
negocio. Módulos Sistema Único de
Información.

versión 0.2.1

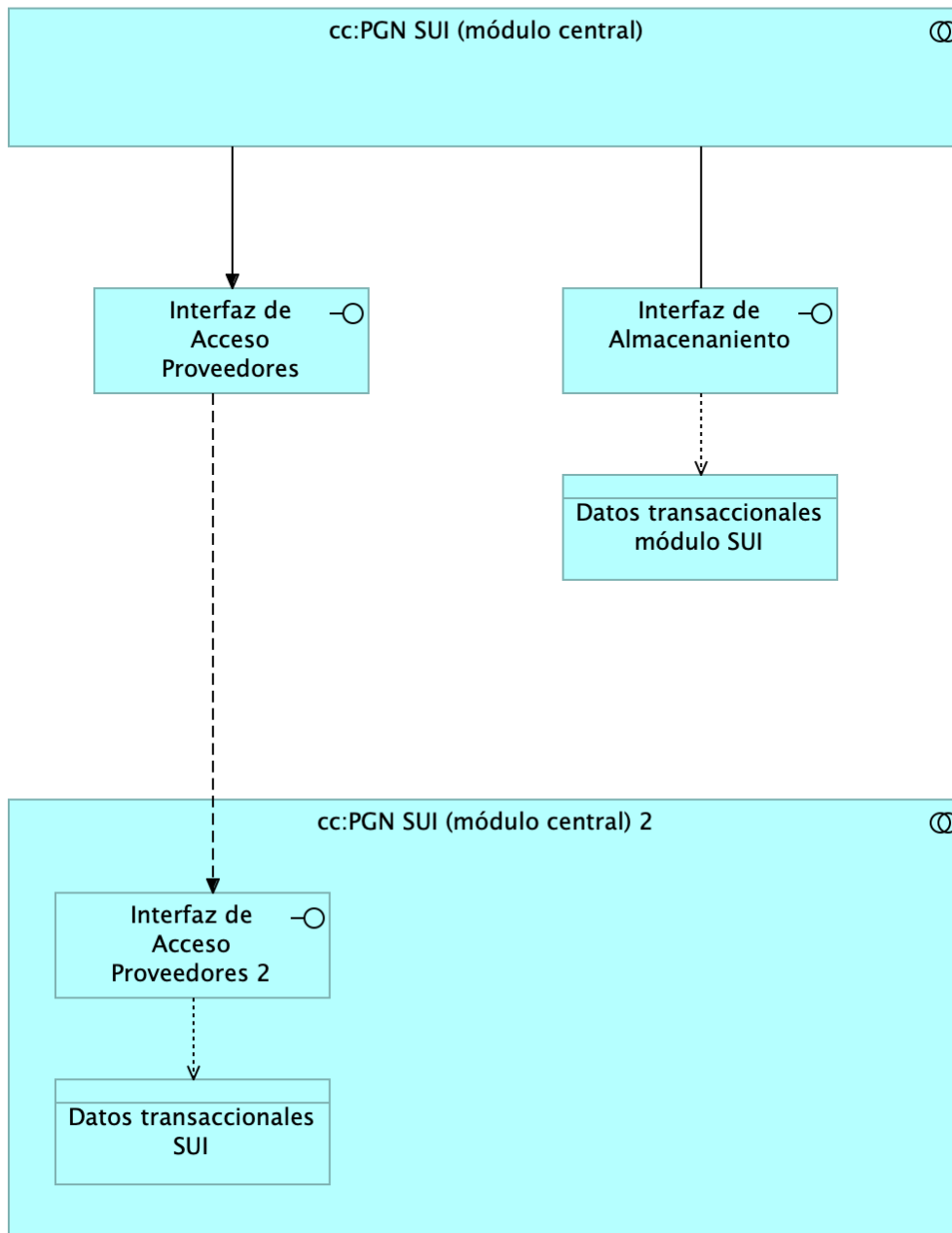


Imagen 12: Vista. Migracion.2d4. Datos Transporte (flujo SUI - SUI)

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

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

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

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 particular 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.	
Interfaz de Acceso Proveedores	application-interface	Interfaz de acceso a los tipos de datos externos al SUI. El patrón de API Externa (reverse proxy) tiene el rol de unir y referir a los datos externos e históricos al SUI Migrado de tal manera que hace transparente la localización y el formato de este tipo de datos.	
Interfaz de Acceso Proveedores 2	application-interface	Interfaz de acceso a los tipos de datos externos al SUI. El patrón de API Externa (reverse proxy) tiene el rol de unir y referir a los datos externos e históricos al SUI Migrado de tal manera que hace transparente la localización y el formato de este tipo de datos.	
Interfaz de Almacenamiento	application-interface	Interfaz de acceso a los repositorio, base de datos relacionales y no jerárquicas. Tipos de datos transaccionales, internos, del SUI.	
Datos transaccionales SUI	data-object		
Datos transaccionales módulo SUI	data-object	Registros de trabajo de un módulo SUI Migrado, 2023.	

Modelo Ontológico

Migracion.2a.a34 Datos Ontológico

PGN. Migración Sistemas Misionales.
Fase 2.

Jerarquización y relacionamiento de
las entidades lógicas (datos de
negocio). Módulos Central Sistema
Único de Información.

versión 0.1

Imagen 13: Vista. Migracion.2a.a34 Datos Ontológico

En construcción.

Catálogo de Elementos

Nombre	Tipo	Descripción	Prop.
--------	------	-------------	-------

Arquitectura de Software: Infraestructura

- [Diagrama de Infraestructura de TI](#)
 - [Migracion.3. Infraestructura](#)
 - [Lineabase.1a.SUI Componentes. Infraestructura](#)
 - [Lineabase.0.SUI Aplicación. Física](#)
 - [Seguridad.2. Lineabase.0.SUI Aplicación](#)
 - [Migracion.6. Migración de datos](#)
- [Documento sobre especificaciones técnicas de infraestructura TI](#)
 - [Lineabase.0.SUI Aplicación. Física](#)

Diagrama de Infraestructura de TI

Migracion.3. Infraestructura

PGN. Migración Sistemas Misionales.
Fase 2.

Diseño de infraestructura. Módulos
Central Sistema Único de
Información, SIU de PGN.

versión 0.2.1

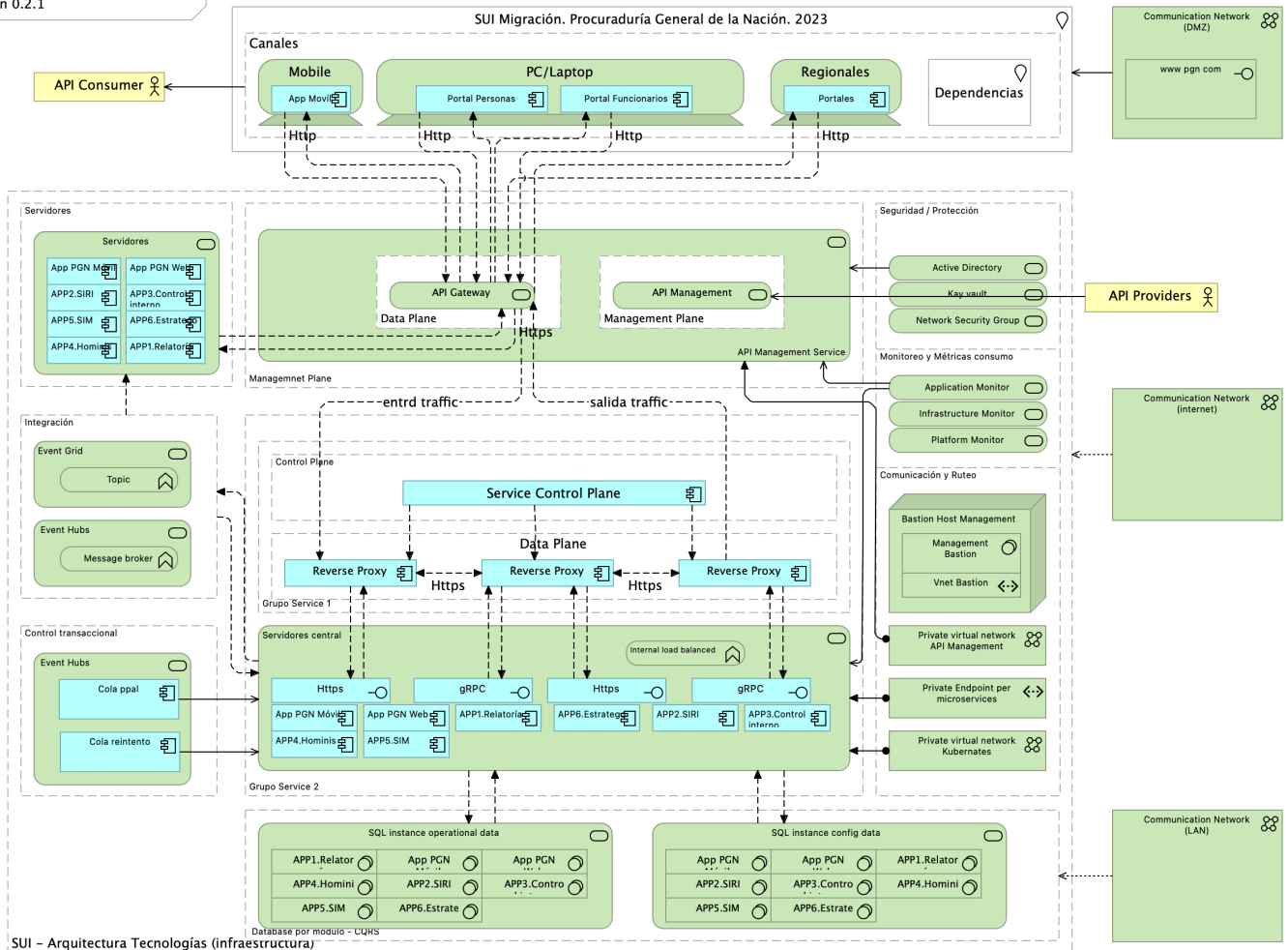


Imagen 14: Vista. Migracion.3. Infraestructura

Identificación de los ítems de infraestructura tecnológica, nodos, redes, cómputo, y almacenamiento relacionado con los módulos del SUI Migrado, 2023.

Representación de Infraestructura

1. Canales
2. Redes
3. Grupo de Servidores
4. Grupo de Servicios
5. Integración
6. Seguridad
7. Almacenamiento
8. Comunicación / Ruteo

Especificaciones Plataformas y Versiones

- Angular, versión 11
- Node Js, versión 14.16
- Net Entity Framework, versión 4.7
- Sequelize, versión 5.3

Especificaciones de Librerías y Dependencias

- Web Server (IIS) role
- Windows Process Activation Service feature
- Microsoft .NET Framework version 3.5
- Microsoft .NET Framework version 4.7.2
- Microsoft SQL Server 2012 Service Pack 4 Native Client
- Microsoft WCF Data Services 5.6
- Microsoft Identity Extensions
- Microsoft Information Protection and Control Client 2.1 (MSIPC)
- Cumulative Update Package 7 for Microsoft AppFabric 1.1 for Windows Server (KB 3092423)
- Visual C++ Redistributable Package for Visual Studio 2012
- Visual C++ Redistributable Package for Visual Studio 2017

Especificaciones Base de Servidores

Servidor de Aplicaciones	Especificaciones del Servidor
Sistema Operativo	Windows Server 2019 Standard or Datacenter x64
RAM	16 GB
CPU	64 Bits, mínimo 4 Cores > 2 Ghz
Discos	C: 120 GB, D: 16 GB
Físico/virtual	Virtual
Roles / Features	Web Server (IIS) role
	Windows Process Activation Service feature
	Microsoft .NET Framework version 3.5

Catálogo de Elementos

Nombre	Tipo	Descripción	Prop.
APP1.Relatoría	application-component	Módulo del SUI. Relatoría pública. Publicación de información de referencia para funcionarios y personas naturales, cientes de la PGN.	

Nombre	Tipo	Descripción	Prop.
APP1.Relatoría	application-component	Módulo del SUI. Relatoría pública. Publicación de información de referencia para funcionarios y personas naturales, cientes de la PGN.	
APP2.SIRI	application-component	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN: SIRI.	
APP2.SIRI	application-component	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN: SIRI.	
APP3.Control interno	application-component	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN: Control Interno.	
APP3.Control interno	application-component	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN: Control Interno.	
APP4.Hominis	application-component	Módulo del SUI. Gestión de capital humano, funcionarios y cargos de representación y libre remoción de la PGN.	
APP4.Hominis	application-component	Módulo del SUI. Gestión de capital humano, funcionarios y cargos de representación y libre remoción de la PGN.	
APP5.SIM	application-component	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN: SIM.	
APP5.SIM	application-component	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN: SIM.	
APP6.Estratego	application-component	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN: Estratego.	

Nombre	Tipo	Descripción	Prop.
APP6.Estratego	application-component	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN: Estratego.	
App Móvil	application-component		
App PGN Móvil	application-component		
App PGN Móvil	application-component		
App PGN Web	application-component		
App PGN Web	application-component		
Cola ppal	application-component		
Cola reintento	application-component		
Portal Funcionarios	application-component		
Portal Personas	application-component		
Portales	application-component		
Reverse Proxy	application-component		
Reverse Proxy	application-component		
Reverse Proxy	application-component		
Service Control Plane	application-component		
Https	application-interface		
Https	application-interface		
gRPC	application-interface		
gRPC	application-interface		
API Consumer	business-actor		
API Providers	business-actor		
Communication Network (DMZ)	communication-network		
Communication Network (LAN)	communication-network		
Communication Network (internet)	communication-network		
Private virtual network API Management	communication-network		
Private virtual network Kubernetes	communication-network		
Mobile	device		
PC/Laptop	device		
Regionales	device		
** Database por módulo - CQRS**	grouping		
Canales	grouping		

Nombre	Tipo	Descripción	Prop.
Comunicación y Ruteo	grouping		
Control Plane	grouping		
Control transaccional	grouping		
Data Plane	grouping		
Data Plane	grouping		
Grupo Service 1	grouping		
Grupo Service 2	grouping		
Integración	grouping		
Management Plane	grouping		
Managemnet Plane	grouping		
Monitoreo y Métricas consumo	grouping		
SUI - Arquitectura Tecnologías (infraestructura)	grouping		
Seguridad / Protección	grouping		
Servidores	grouping		
Dependencias	location		
SUI Migración. Procuraduría General de la Nación. 2023	location		
Bastion Host Management	node		
Private Endpoint per microservices	path		
Vnet Bastion	path		
APP1.Relatoría	system-software		
APP1.Relatoría	system-software		
APP2.SIRI	system-software		
APP2.SIRI	system-software		
APP3.Control interno	system-software		
APP3.Control interno	system-software		
APP4.Hominis	system-software		
APP4.Hominis	system-software		
APP5.SIM	system-software		
APP5.SIM	system-software		
APP6.Estratego	system-software		
APP6.Estratego	system-software		
App PGN Móvil	system-software		

Nombre	Tipo	Descripción	Prop.
App PGN Móvil	system-software		
App PGN Web	system-software		
App PGN Web	system-software		
Management Bastion	system-software		
Internal load balanced	technology-function		
Message broker	technology-function		
Topic	technology-function		
www pgn com	technology-interface		
** Event Hubs**	technology-service		
** Event Hubs**	technology-service		
API Gateway	technology-service		
API Management	technology-service		
API Management Service	technology-service		
Active Directory	technology-service		
Application Monitor	technology-service		
Event Grid	technology-service		
Infrastructure Monitor	technology-service		
Kay vault	technology-service		
Network Security Group	technology-service		
Platform Monitor	technology-service		
SQL instance config data	technology-service		
SQL instance operational data	technology-service		
Servidores	technology-service		
Servidores central	technology-service		

Lineabase.1a.SUI Componentes. Infraestructura

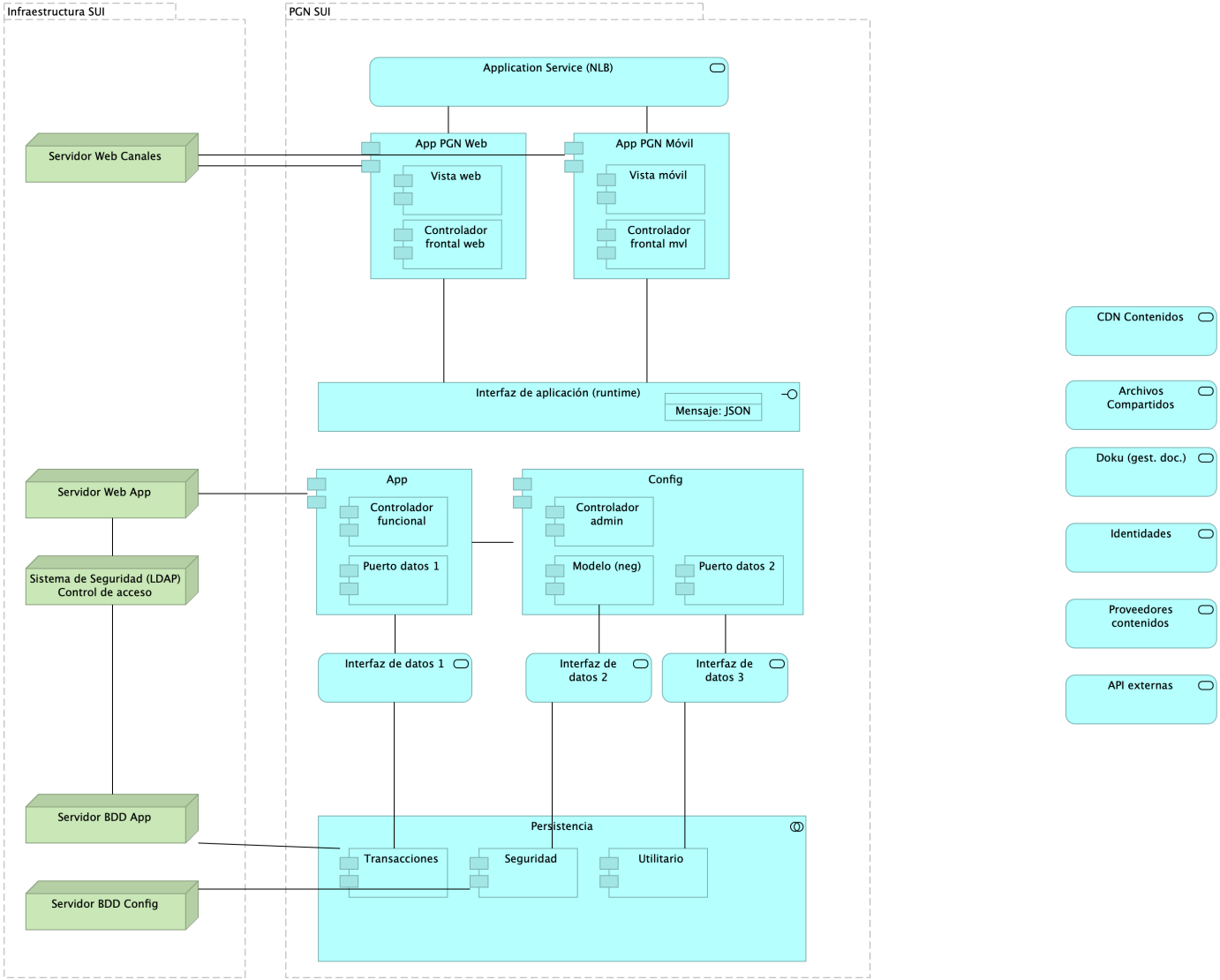


Imagen 15: Vista. Lineabase.1a.SUI Componentes. Infraestrctura

Relación de dependencias de infraestructura con los servicios que integran el modelo de aplicación de SUI Migrado, 2023.

Elementos de Infraestructura SUI Migrado

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

Catálogo de Elementos

Nombre	Tipo	Descripción	Prop.
Persistencia	application-collaboration		
App	application-component		plataforma: node Js brecha: 100

Nombre	Tipo	Descripción	Prop.
App PGN Móvil	application-component		<i>plantilla:</i> element-md-bold <i>brecha:</i> 100
App PGN Web	application-component		<i>plataforma:</i> angular 11 <i>brecha:</i> 100
Config	application-component		<i>plataforma:</i> cs
Controlador admin	application-component		<i>plataforma:</i> cs
Controlador frontal mvl	application-component		<i>plataforma:</i> 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.	<i>plataforma:</i> js
Controlador funcional	application-component		<i>plataforma:</i> js
Modelo (neg)	application-component		<i>plataforma:</i> cs
Puerto datos 1	application-component		<i>plataforma:</i> js
Puerto datos 2	application-component		<i>plataforma:</i> cs
Seguridad	application-component		<i>plataforma:</i> sql <i>brecha:</i> 100
Transacciones	application-component		<i>plataforma:</i> sql <i>brecha:</i> 100
Utilitario	application-component		<i>plataforma:</i> no-sql
Vista móvil	application-component		<i>plataforma:</i> js
Vista web	application-component		<i>plataforma:</i> 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"	<i>plataforma:</i> angular 11
API externas	application-service		

Nombre	Tipo	Descripción	Prop.
Application Service (NLB)	application-service		<i>plataforma:</i> angular 11 <i>brecha:</i> 100
Archivos Compartidos	application-service		
CDN Contenidos	application-service		<i>brecha:</i> 100
Doku (gest. doc.)	application-service		<i>brecha:</i> 100
Identidades	application-service		
Interfaz de datos 1	application-service		
Interfaz de datos 2	application-service		
Interfaz de datos 3	application-service		
Proveedores contenidos	application-service		<i>brecha:</i> 100
Mensaje: JSON	data-object		
Infraestructura SUI	grouping	Soporte de infraestructura a los componentes del SUI Migración. Servidores y ambientes de cómputo para la ejecución del software base de los componentes misionales del SUI de PGN.	
PGN SUI	grouping	Esta vista presenta y describe los ítems de arquitectura del SUI Migrado que requieren licenciamiento para operar y cumplir con el objetivo principal de la migración que es la centralización de los conceptos misionales: concentrar los conceptos misionales en componentes aislados. Los elementos realtados en verde en el diagrama incurren en una renta, bien sea, o por consumo de cómputo en la nube de Microsoft, o por el costo de una licencia de uso. Por ejemplo, en el caso del servidor de reporte del SUI Migrado, es requerida una licencia de uso Power BI Pro, de pago mensual.	
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.	

Nombre	Tipo	Descripción	Prop.
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.	
Sistema de Seguridad (LDAP) Control de acceso	node	Sistema de autenticación del directorio activo.	

Lineabase.0.SUI Aplicación. Física

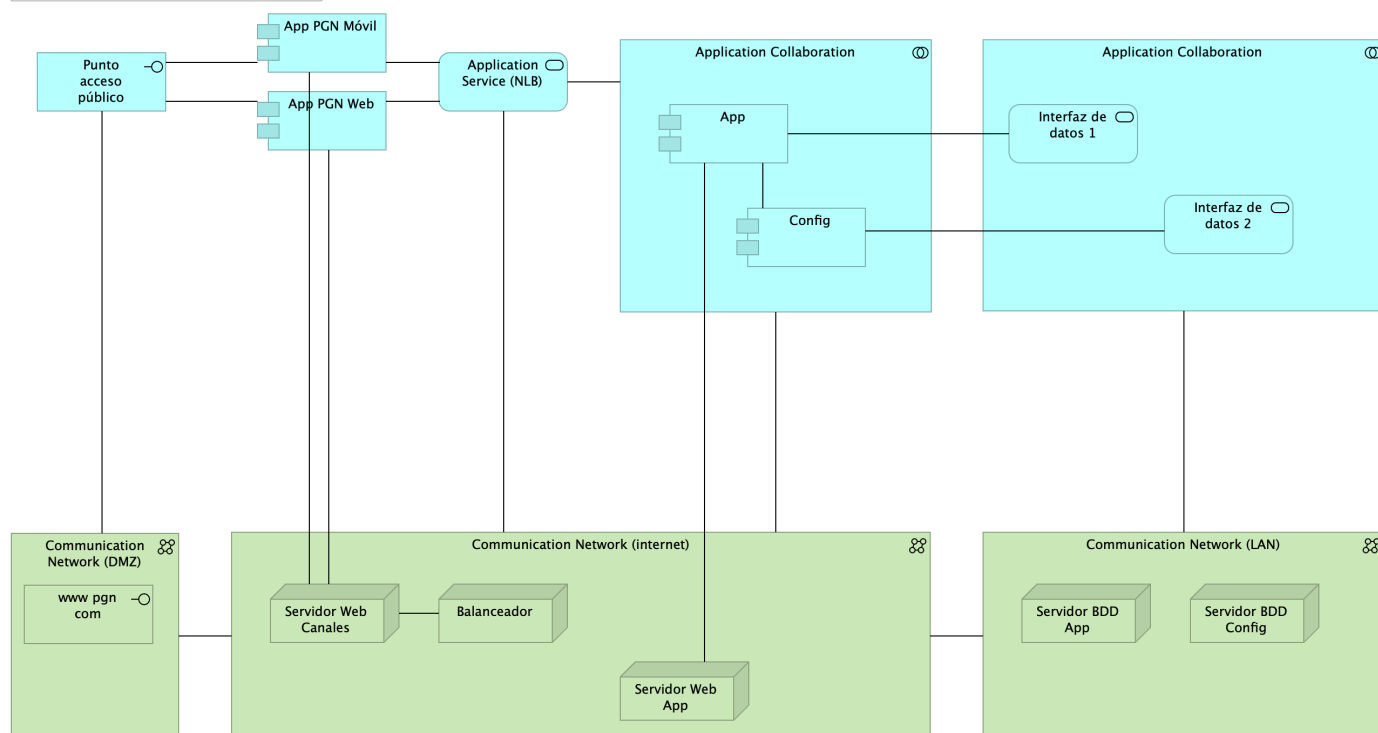


Imagen 16: Vista. Lineabase.0.SUI Aplicación. Física

Procuraduría General de la Nación (PGN), módulo Sistema Único de Información (SUI), 2023. Elementos físicos que soportan a la aplicación doc Sistema Único de Información (SUI) 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 de Arquitectura

Con una arquitectura orientada a servicios Sistema Único de Información (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

Especificaciones Plataformas y Versiones

- Angular, versión 11
- Node Js, versión 14.16
- Net Entity Framework, versión 4.7
- Sequelize, versión 5.3

Especificaciones de Librerías y Dependencias

- Web Server (IIS) role
- Windows Process Activation Service feature
- Microsoft .NET Framework version 3.5
- Microsoft .NET Framework version 4.7.2
- Microsoft SQL Server 2012 Service Pack 4 Native Client
- Microsoft WCF Data Services 5.6
- Microsoft Identity Extensions
- Microsoft Information Protection and Control Client 2.1 (MSIPC)
- Cumulative Update Package 7 for Microsoft AppFabric 1.1 for Windows Server (KB 3092423)
- Visual C++ Redistributable Package for Visual Studio 2012
- Visual C++ Redistributable Package for Visual Studio 2017

Especificaciones Base de Servidores

Servidor de Aplicaciones	Especificaciones del Servidor
Sistema Operativo	Windows Server 2019 Standard or Datacenter x64
RAM	16 GB
CPU	64 Bits, mínimo 4 Cores > 2 Ghz
Discos	C: 120 GB, D: 16 GB
Físico/virtual	Virtual
Roles / Features	Web Server (IIS) role
	Windows Process Activation Service feature
	Microsoft .NET Framework version 3.5

Catálogo de Elementos

Nombre	Tipo	Descripción	Prop.
Application Collaboration	application-collaboration		
Application Collaboration	application-collaboration		
App	application-component		<i>plataforma:</i> node js <i>brecha:</i> 100
App PGN Móvil	application-component		<i>plantilla:</i> element-md-bold <i>brecha:</i> 100
App PGN Web	application-component		<i>plataforma:</i> angular 11 <i>brecha:</i> 100
Config	application-component		<i>plataforma:</i> cs
Punto acceso público	application-interface	URL tipo C HTTP	
Application Service (NLB)	application-service		<i>plataforma:</i> angular 11 <i>brecha:</i> 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		

Seguridad.2. Lineabase.0.SUI Aplicación

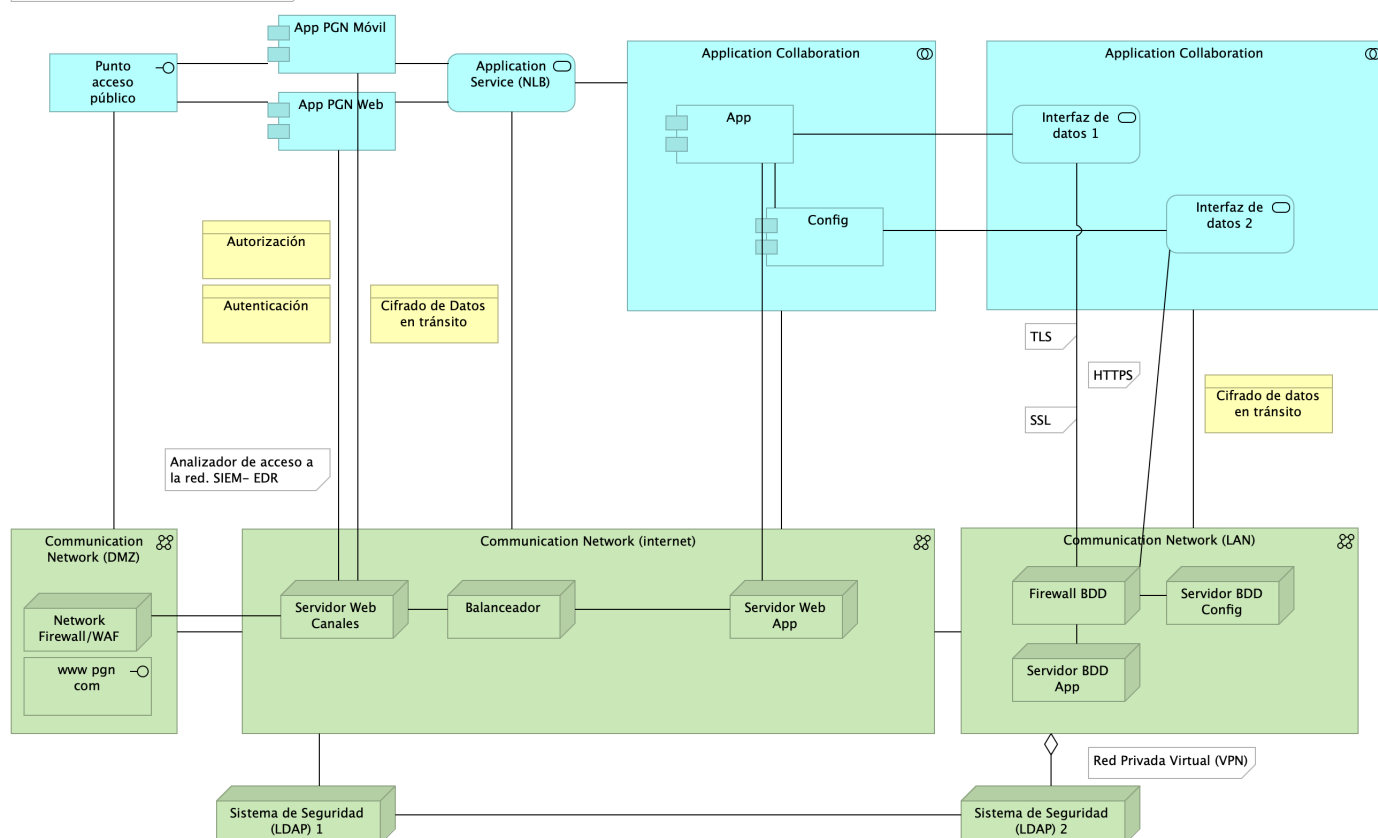


Imagen 17: Vista. Seguridad.2. Lineabase.0.SUI Aplicación

Metodología Seguridad Sistema Único de Información (SUI)

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 de Creación de Usuarios e Identificación de Privilegios

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)".

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.

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 Seguridad de la Información Confidencialidad e integridad, asimismo reducir los riesgos de la información mediante la ayuda de Técnicas Criptográficas.

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 así evitar manipulación de información confidencial. La Seguridad que brinda SSL, da garantía para acceder a los aplicativos de PNG.

Cómo implementar certificados SSL

Podrán 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 envío de la información, proporcionando una autenticación sólida, restringiendo la manipulación, interceptación y alteración de mensajes.

La última versión del TLS es la 1.3

Representación Arquitectónica

Con una arquitectura orientada a servicios SUI recopilamos:

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

Catálogo de Elementos

Nombre	Tipo	Descripción	Prop.
Application Collaboration	application-collaboration		
Application Collaboration	application-collaboration		
App	application-component		<i>plataforma:</i> node js <i>brecha:</i> 100
App PGN Móvil	application-component		<i>plantilla:</i> element-md-bold <i>brecha:</i> 100
App PGN Web	application-component		<i>plataforma:</i> angular 11 <i>brecha:</i> 100
Config	application-component		<i>plataforma:</i> cs
Punto acceso público	application-interface	URL tipo C HTTP	
Application Service (NLB)	application-service		<i>plataforma:</i> angular 11 <i>brecha:</i> 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		
Communication Network (DMZ)	communication-network		
Communication Network (LAN)	communication-network		
Communication Network (internet)	communication-network		
Balanceador	node		
Firewall BDD	node		<i>brecha:</i> 100

Nombre	Tipo	Descripción	Prop.
Network Firewall/WAF	node		<i>brecha: 100</i>
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.	
Sistema de Seguridad (LDAP) 1	node	Sistema de Seguridad (LDAP) 1. Control de acceso internet, La autenticación podrá estar integrada con el directorio activo, a partir de la generación de código para el ingreso con 2FA, que podrá generar un código la plataforma de correo corporativo, el cual solicitará el código de autenticación y una vez ingresado podrá redirigir al sitio.	<i>brecha: 100</i>

Nombre	Tipo	Descripción	Prop.
Sistema de Seguridad (LDAP) 2	node	Sistema de Seguridad (LDAP) 2. Control de acceso internet, La solución se podrá integrar con el directorio activo, a partir de la generación del 2FA, que podrá generar un código por desde la plataforma de office 365, el cual solicitará el código de autenticación y una vez ingresado podrá acceder al sitio.	brecha: 100
www pgn com	technology-interface		

Migracion.6. Migración de datos

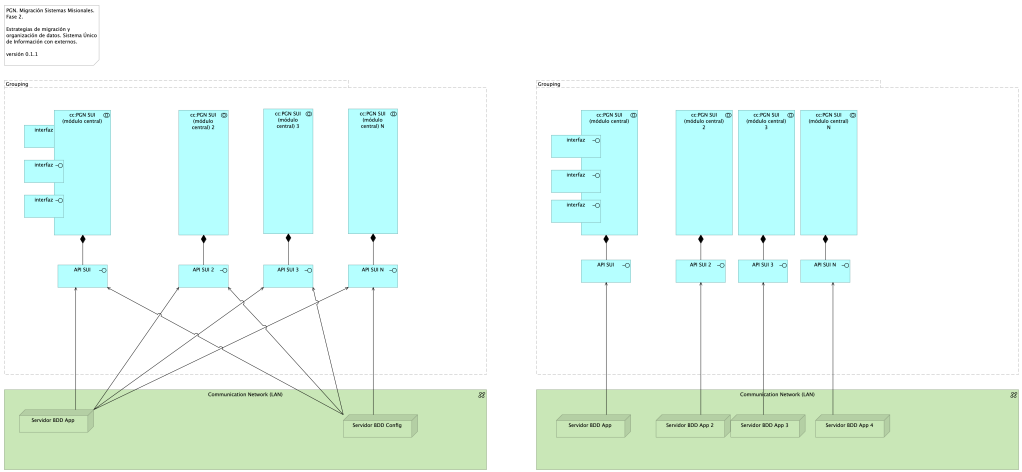


Imagen 18: Vista. Migracion.6. Migración de datos

Modelo de acceso a datos de negocio del SIM.

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

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

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

Catálogo de Elementos

Nombre	Tipo	Descripción	Prop.
--------	------	-------------	-------

Nombre	Tipo	Descripción	Prop.
cc:PGN SUI (módulo central)	application-collaboration	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN.	
cc:PGN SUI (módulo central)	application-collaboration	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN.	
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) 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) 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:PGN SUI (módulo central) N	application-collaboration	Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN.	
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.	

Nombre	Tipo	Descripción	Prop.
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 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.	
API SUI N	application-interface	API de representación del módulo. Centralización de la comunicación con otros módulos del SUI migrado.	
interfaz	application-interface		
interfaz	application-interface		
interfaz	application-interface		
interfaz	application-interface		
interfaz	application-interface		
interfaz	application-interface		
Communication Network (LAN)	communication-network		
Communication Network (LAN)	communication-network		
Grouping	grouping		
Grouping	grouping		
Servidor BDD App	node	Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 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 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.	

Nombre	Tipo	Descripción	Prop.
Servidor BDD App 2	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 App 3	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 App 4	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.	

Documento sobre especificaciones técnicas de infraestructura TI

Lineabase.0.SUI Aplicación. Física

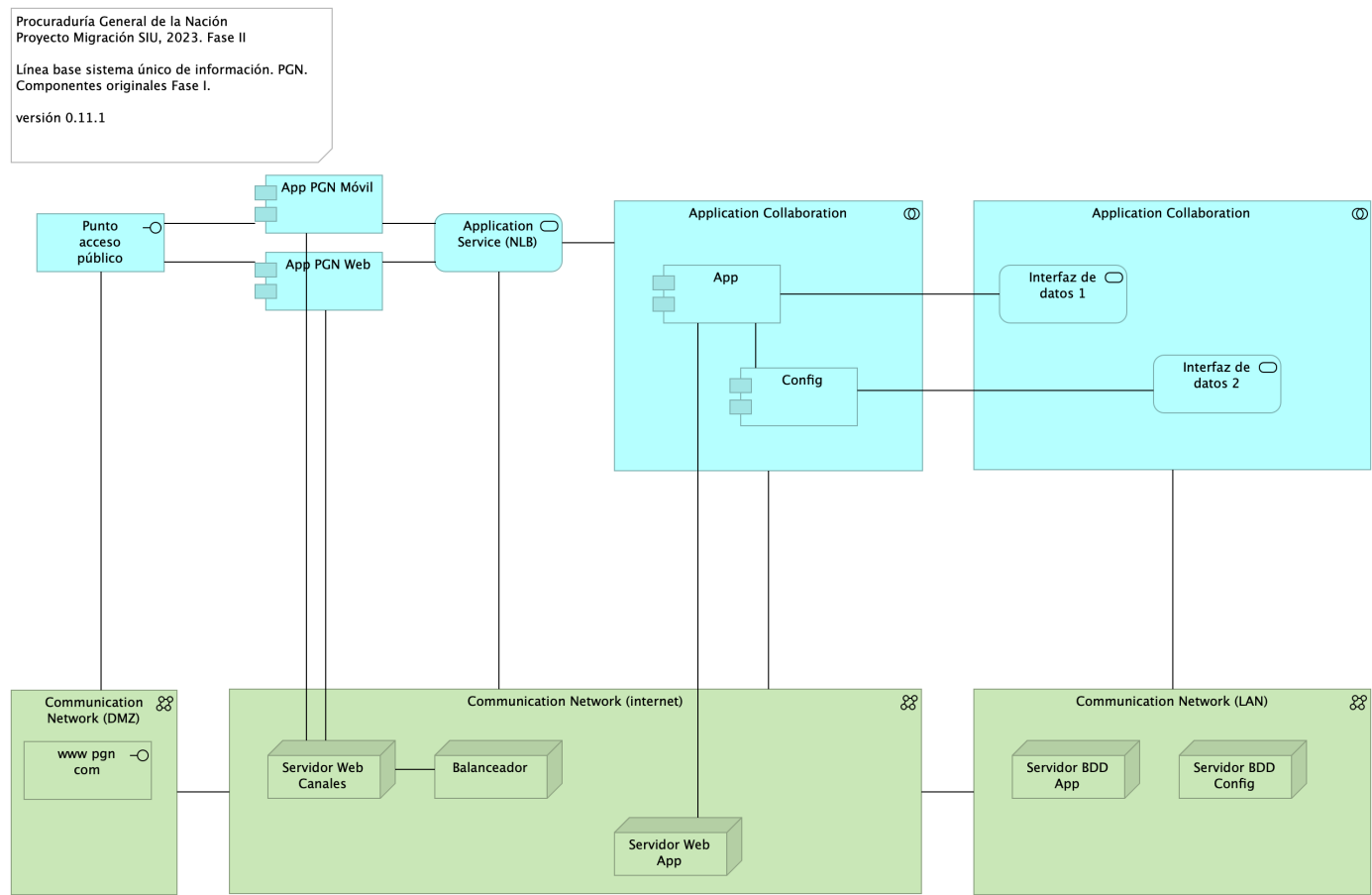


Imagen 19: Vista. Lineabase.0.SUI Aplicación. Física

Procuraduría General de la Nación (PGN), módulo Sistema Único de Información (SUI), 2023. Elementos físicos que soportan a la aplicación doc Sistema Único de Información (SUI) 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 de Arquitectura

Con una arquitectura orientada a servicios Sistema Único de Información (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

Especificaciones Plataformas y Versiones

- Angular, versión 11
- Node Js, versión 14.16
- Net Entity Framework, versión 4.7
- Sequelize, versión 5.3

Especificaciones de Librerías y Dependencias

- Web Server (IIS) role
- Windows Process Activation Service feature
- Microsoft .NET Framework version 3.5
- Microsoft .NET Framework version 4.7.2
- Microsoft SQL Server 2012 Service Pack 4 Native Client
- Microsoft WCF Data Services 5.6
- Microsoft Identity Extensions
- Microsoft Information Protection and Control Client 2.1 (MSIPC)
- Cumulative Update Package 7 for Microsoft AppFabric 1.1 for Windows Server (KB 3092423)
- Visual C++ Redistributable Package for Visual Studio 2012
- Visual C++ Redistributable Package for Visual Studio 2017

Especificaciones Base de Servidores

Servidor de Aplicaciones	Especificaciones del Servidor
Sistema Operativo	Windows Server 2019 Standard or Datacenter x64
RAM	16 GB
CPU	64 Bits, mínimo 4 Cores > 2 Ghz
Discos	C: 120 GB, D: 16 GB
Físico/virtual	Virtual
Roles / Features	Web Server (IIS) role
	Windows Process Activation Service feature
	Microsoft .NET Framework version 3.5

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

Nombre	Tipo	Descripción	Prop.
App PGN Web	application-component		<i>plataforma:</i> angular 11 <i>brecha:</i> 100
Config	application-component		<i>plataforma:</i> cs
Punto acceso público	application-interface	URL tipo C HTTP	
Application Service (NLB)	application-service		<i>plataforma:</i> angular 11 <i>brecha:</i> 100
Interfaz de datos 1	application-service		
Interfaz de datos 2	application-service		
Communication Network (DMZ)	communication-network		
Communication Network (LAN)	communication-network		
Communication Network (internet)	communication-network		
Balanceador	node		
Servidor BDD App	node	Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz. Discos SO C: 126 GB, Backup E: 511 GB, SQL Data F: 510 GB, SQL Log G: 510 GB, TempDB G: 63.6 GB.	
Servidor BDD Config	node	Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz. Discos SO C: 80 GB, Backup E: 250 GB, SQL Data F: 250 GB, SQL Log G: 250 GB, TempDB G: 30 GB.	
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		

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

24. Debe cumplir con todos los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la "Guía de desarrollo OWASP" y "OWAS Cheat Sheet".

Referencias

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

1. **Softgic. Proyecto de mejoramiento SUI 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/>