


Documento de Arquitectura Migración Funcional PGN SIU

Los productos de esta etapa, Migración Funcional SIU, Contrato 078-2023, ([Web](#)) están basados en el resultado de la Fase 1 del proyecto PGN SIU del 2022, [Sharepoint Softgic@10c5e4b](#) del August 31, 2023.

Versión del producto 1.10c5e4b de 31 Aug 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.

Control de Cambios

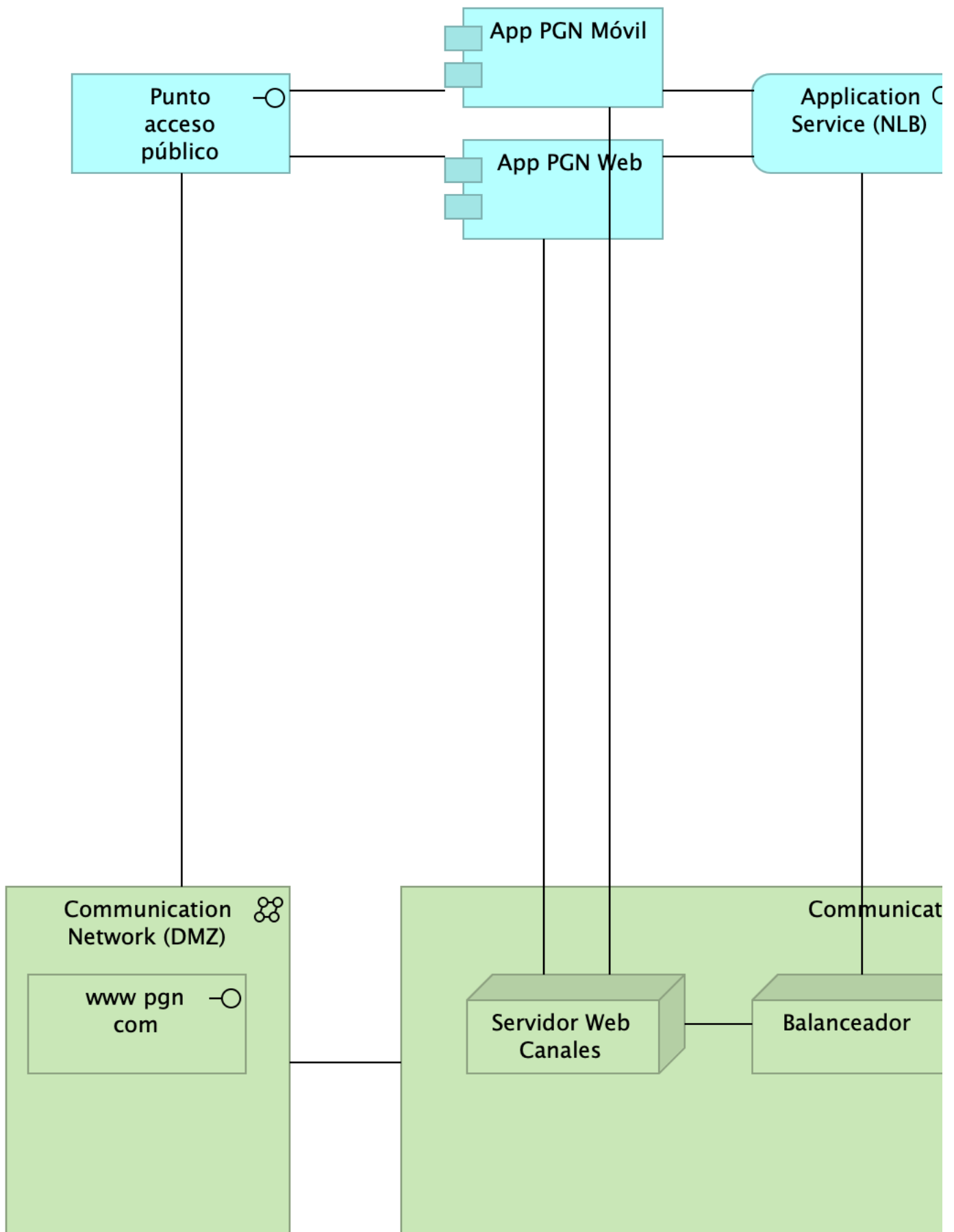
Tema	078-2023 Fase 2, PGN Migración Funcional SIU
Palabras clave	SIU, Softgic, PGN, Análisis de brecha, GAP, Comparativa
Autor	
Fuente	
Versión	1.10c5e4b del 31 Aug 2023
Vínculos	N003a Vista Segmento PGN SIU

Documento de Arquitectura Migración SIU

- [Línea Base PGN SIU](#)
 - [Lineabase.0.SIU aplicación](#)
 - [Lineabase.1.SIU componente](#)
 - [Lineabase.1a.SIU componente](#)
 - [Lineabase.2.Portal](#)
 - [Riesgos.1](#)
- [Arquitectura Migración PGN SIU](#)
 - [Migracion.1.SIU modulos](#)

Línea Base PGN SIU

Lineabase.0.SIU aplicación



Representación Arquitectónica

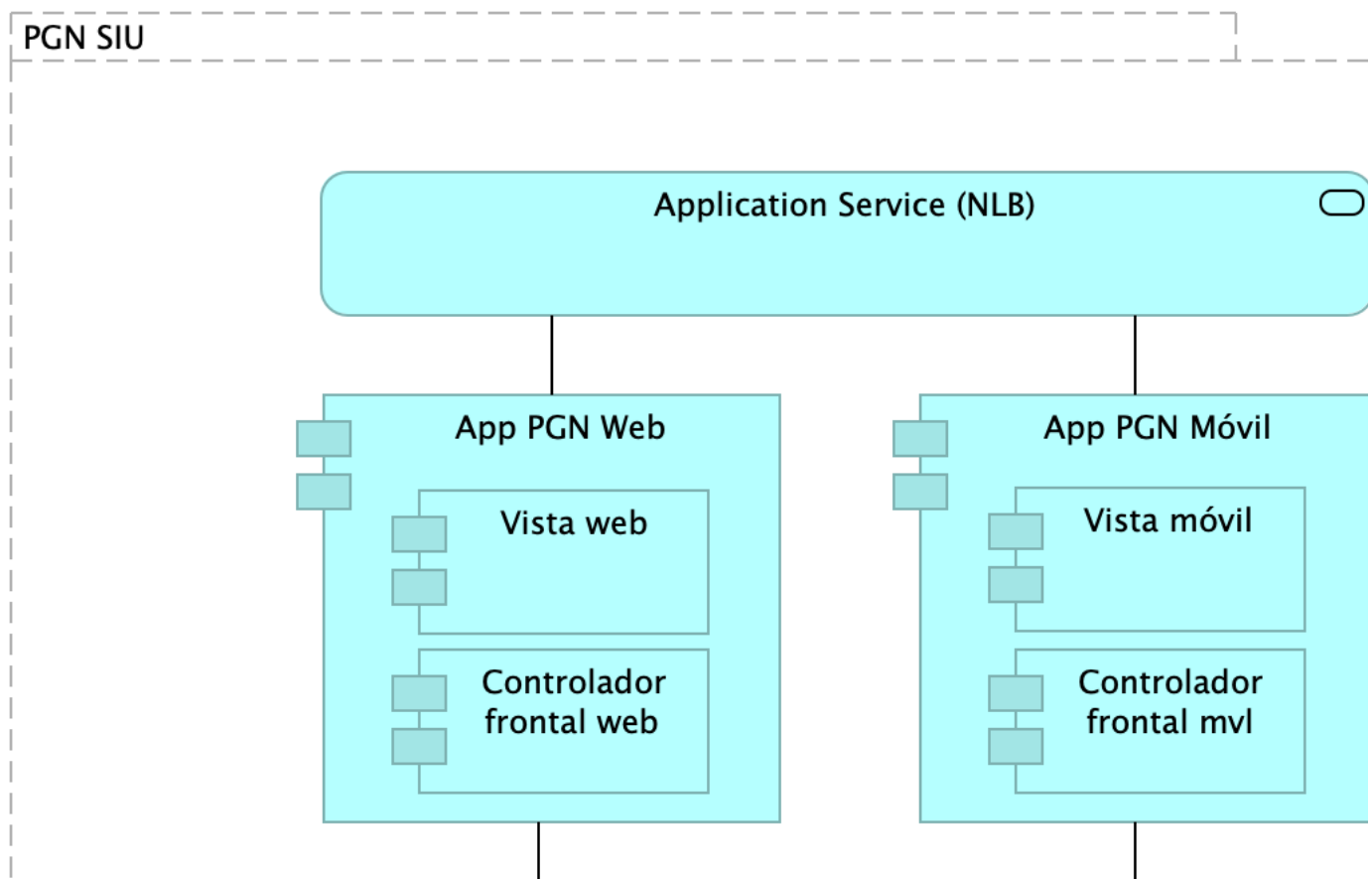
Con una arquitectura orientada a servicios SUI recopila:

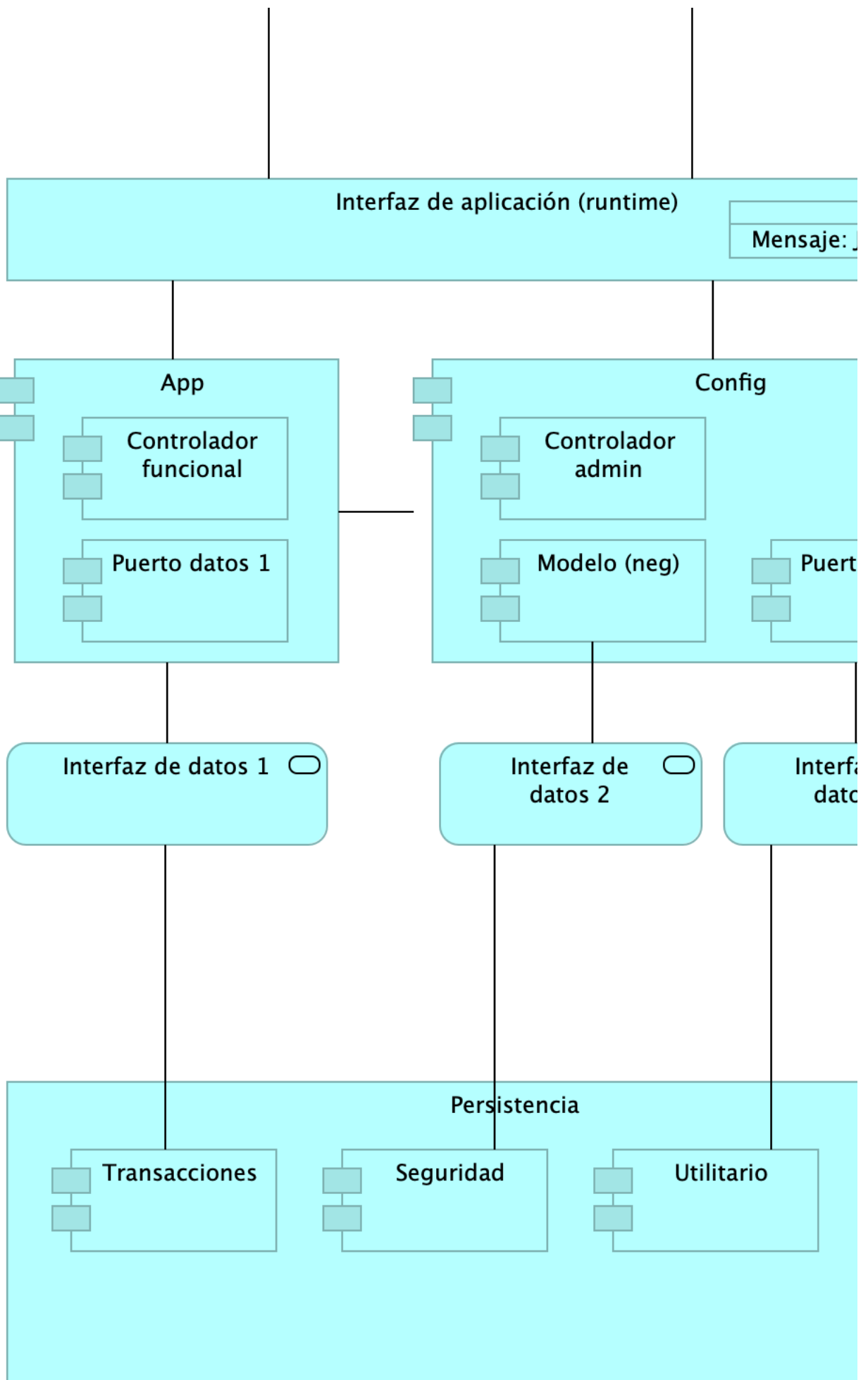
1. Runtime: Es el servicio que interactúa con el usuario final (GUI) elaborado en Angular 11
2. API Tx: Servicio api rest base node encargado de realizar las transacciones básicas CRUD
3. API Config / Seguridad. Servicio Web API .Net Framework encargado de gestionar características con la autenticación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

Catálogo de Elementos

Name	Type	Description	Properties
Application Collaboration	application-collaboration		
Application Collaboration	application-collaboration		
App	application-component		plataforma: node Js
App PGN Móvil	application-component		
App PGN Web	application-component		plataforma: angular 11
Config	application-component		plataforma: cs
Punto acceso público	application-interface		
Application Service (NLB)	application-service		plataforma: angular 11
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		
Servidor BDD Config	node		
Servidor Lappiz	node		
Servidor Web App	node		
Servidor Web Canales	node		
www pgn com	technology-interface		

Lineabase.1.SIU componente





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

Cuatro paquetes con tecnologías respectivas 1. Angular 11 (Web) 1. API Transaccional (Node Js) 1. API Config (C#) 1. Persistencia (SQL)

Asuntos de la Migración: * Estrategia CMS central * Motor de búsqueda * Estatego como BI * Conciliación y Doku * Gestión de sesiones / caducidad

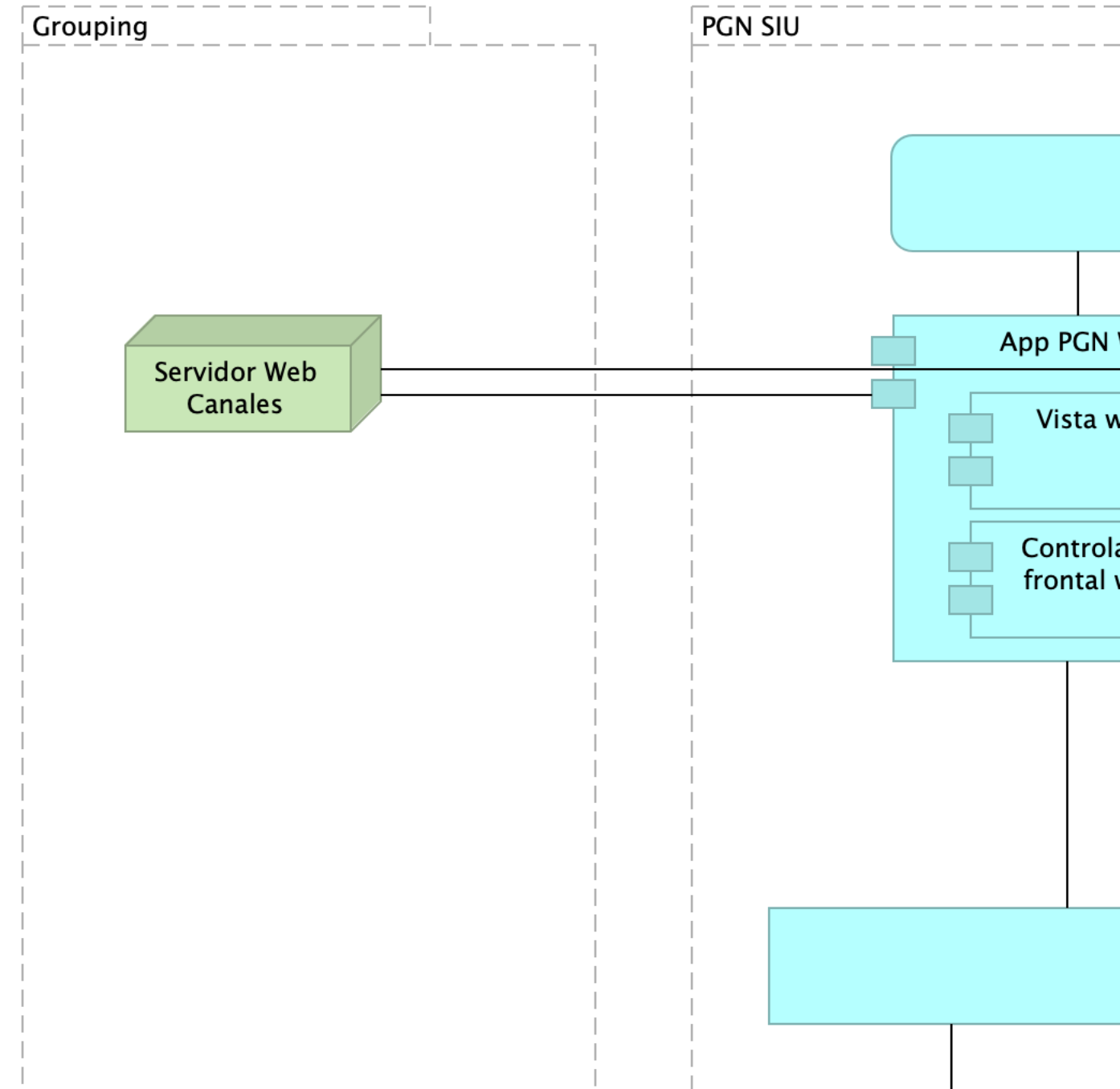
Catálogo de Elementos

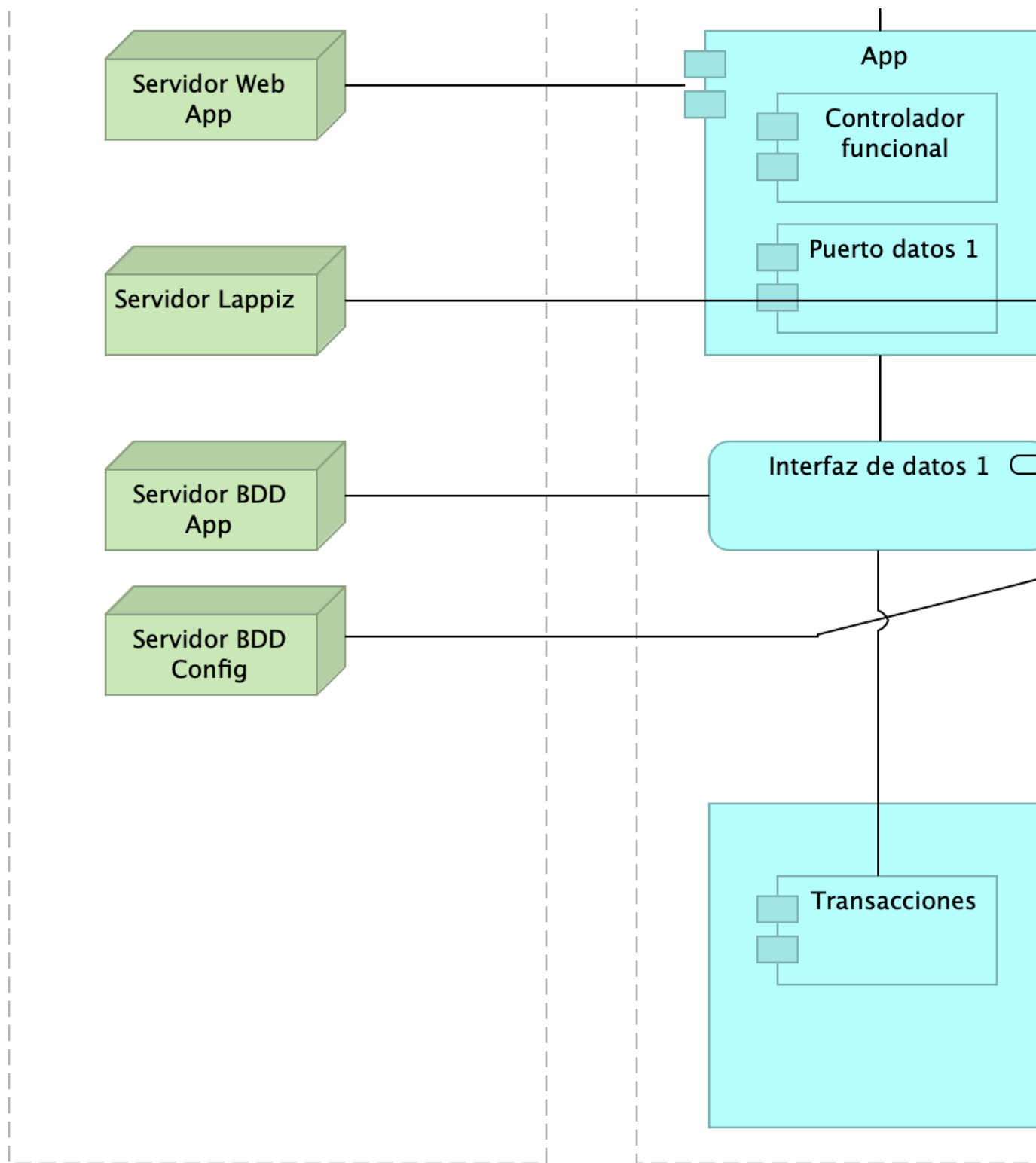
Name	Type	Description	Properties
Persistencia	application-collaboration		
App	application-component		plataforma: node Js
App PGN Móvil	application-component		
App PGN Web	application-component		plataforma: angular 11
Config	application-component		plataforma: cs
Controlador admin	application-component		plataforma: cs
Controlador frontal mvl	application-component		plataforma: js
Controlador frontal web	application-component		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
Transacciones	application-component		plataforma: sql
Utilitario	application-component		plataforma: no-sql
Vista móvil	application-component		plataforma: js
Vista web	application-component		plataforma: html
Interfaz de aplicación (runtime)	application-interface		plataforma: angular 11
API externas	application-service		
Application Service (NLB)	application-service		plataforma: angular 11
Archivos Compartidos	application-service		
CDN Contenidos	application-service		
Doku (gest. doc.)	application-service		
Identidades	application-service		
Interfaz de datos 1	application-service		
Interfaz de datos 2	application-service		
Interfaz de datos 3	application-service		
Proveedores contenidos	application-service		
Mensaje: JSON	data-object		
PGN SIU	grouping		
RQR. Administrativos	requirement		
RQR. Funcionales	requirement		
RQR. Ingeniería	requirement		
RQR. Seguridad	requirement	<p>1. Las soluciones deben dar cumplimiento a las políticas institucionales del sistema de gestión de seguridad de la información establecidas por la entidad que busca garantizar la confidencialidad, integridad y disponibilidad de la información que se genera, procesa, almacena y/o transmite en los sistemas de Información de la Entidad.</p> <p>1. Las soluciones de automatización de procesos a implementar deben permitir la Gestión de Seguridad de Usuarios, grupos de usuarios y asignación de Roles y perfiles de usuarios, permitiendo asociar las acciones disponibles en la solución con respecto a roles de usuario, permitiendo parametrizar las funcionalidades que cada actor puede usar en la solución.</p> <p>1. Un usuario puede estar asociado a uno o más roles, de tal manera que los menús de navegación de la solución se muestran o despliegan dependiendo de las acciones asociadas a cada rol de usuario, permitiendo así que cuando el usuario es</p>	

Name	Type	Description	Properties
		<p>autenticado correctamente, la solución verifica los roles que tiene activos para otorgarle únicamente las acciones autorizadas.</p> <p>1. El diseño de la solución debe definir los criterios necesarios para asegurar la trazabilidad y auditoría sobre las acciones de creación, actualización, modificación o borrado de los componentes de información, de tal manera que la solución debe permitirle al administrador de la solución parametrizar las tablas y eventos que pueden auditarse.</p> <p>1. Las soluciones deben tener en cuenta mecanismos que aseguren el registro histórico para poder mantener la trazabilidad de las acciones realizadas por los usuarios, contemplando el registro de auditoría que contiene información de fecha y hora, identificación del registro, tabla afectada, descripción del evento, tipo de evento, usuario que realiza la acción, identificación de sesión y dirección IP del usuario que efectuó la transacción.</p> <p>1. La solución debe proveer una consulta que permita a un usuario con los privilegios asignados, consultar los registros de auditoría, aplicando criterios de filtro (usuario, maquina, rango de fechas y tipo de operación).</p> <p>1. Las soluciones deben integrarse con LDAP – (Lightweight Directory Access Protocol) para los procesos de inicio de sesión y autenticación. La solución debe soportar la integración Nativa con Active Directory de Microsoft. Para usuarios externos el mecanismo de autorización, autenticación y acceso será controlado a través del modelo de seguridad de la solución (no habrá autenticación para usuarios externos).</p> <p>1. Las soluciones deben cumplir con los lineamientos de seguridad relacionados a su utilización a través de redes públicas y privadas, garantizando la confidencialidad e integridad de la información y acceso a ella.</p> <p>1. Debe evidenciar que, a través de pruebas de vulnerabilidad, garantiza la seguridad de la información. Estas pruebas deben suministrar evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad.</p> <p>1. Debe incluir un mecanismo de cifrado de los datos que se transportan entre los diferentes componentes tecnológicos y los datos sensibles de la base de datos que representen un alto nivel de confidencialidad.</p> <p>1. A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio).</p> <p>1. Debe contemplar el cumplimiento de la normatividad vigente en cuanto a protección de datos personales y debe permitir el manejo de excepciones.</p> <p>1. Para los casos que aplique se debe permitir el manejo de certificados y/o firmas digitales en los documentos que así se definan para efectos de aprobación y digitalización.</p> <p>1. Debe contemplar las prácticas de desarrollo seguro de aplicaciones y/o implementación segura de productos, para su naturaleza Web based.</p> <p>1. Debe funcionar sobre protocolo SSL (certificados internos de la entidad cuando los sistemas de información sean internas y certificados validos públicamente cuando los sistemas de información estén expuestas a internet).</p> <p>1. Debe entregar un procedimiento para el respaldo de la información de acuerdo con las necesidades de la entidad.</p> <p>1. Debe incluir uso de criptografía para transacciones y/o campos sensibles según lo indiquen las normas vigentes y las necesidades específicas del negocio de acuerdo como lo determine la entidad.</p> <p>1. Debe contemplar un modelo de datos que garantice base de datos única para evitar que se pueda presentar duplicidad de información.</p>	

Name	Type	Description	Properties
		<p>1. En la información confidencial solo puede ser consultada por los perfiles autorizados e igualmente restringir documentos de consulta según los privilegios o permisos asociados.</p> <p>1. A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio).</p> <p>1. Debe cerrar las transacciones luego de máximo 10 minutos de inactividad.</p> <p>1. Debe incluir controles de bloqueo de cuenta después de un máximo de 5 intentos erróneos a fin de evitar ataques de fuerza bruta.</p> <p>1. Debe evidenciar el resultado positivo frente apruebas de ethical hacking, análisis de vulnerabilidades, carga, estrés y desempeño antes de la puesta en operación de acuerdo con los lineamientos de la entidad.</p> <p>1. Debe cumplir con todos los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la “Guía de desarrollo OWASP” y “OWAS Cheat Sheet”.</p>	

Lineabase.1a.SIU componente





Dependencias entre los servicios que integran la aplicación de SUI.

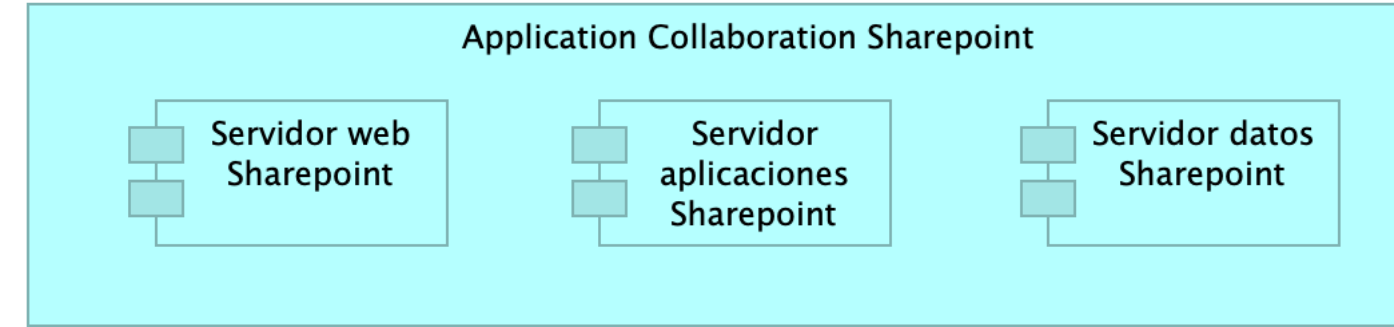
4 paquetes con tecnologías respectivas Angular 11 (Web), Api Transaccional (Node Js) y Api Config (C#) y el alojamiento de datos.

Catálogo de Elementos

Name	Type	Description	Properties
Persistencia	application-collaboration		
App	application-component		plataforma: node Js
App PGN Móvil	application-component		
App PGN Web	application-component		plataforma: angular 11
Config	application-component		plataforma: cs
Controlador admin	application-component		plataforma: cs
Controlador frontal mvl	application-component		plataforma: js

Name	Type	Description	Properties
Controlador frontal web	application-component		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
Transacciones	application-component		plataforma: sql
Utilitario	application-component		plataforma: no-sql
Vista móvil	application-component		plataforma: js
Vista web	application-component		plataforma: html
Interfaz de aplicación (runtime)	application-interface		plataforma: angular 11
API externas	application-service		
Application Service (NLB)	application-service		plataforma: angular 11
Archivos Compartidos	application-service		
CDN Contenidos	application-service		
Doku (gest. doc.)	application-service		
Identidades	application-service		
Interfaz de datos 1	application-service		
Interfaz de datos 2	application-service		
Interfaz de datos 3	application-service		
Proveedores contenidos	application-service		
Mensaje: JSON	data-object		
Grouping	grouping		
PGN SIU	grouping		
Servidor BDD App	node		
Servidor BDD Config	node		
Servidor Lappiz	node		
Servidor Web App	node		
Servidor Web Canales	node		

Linebase.2.Portal



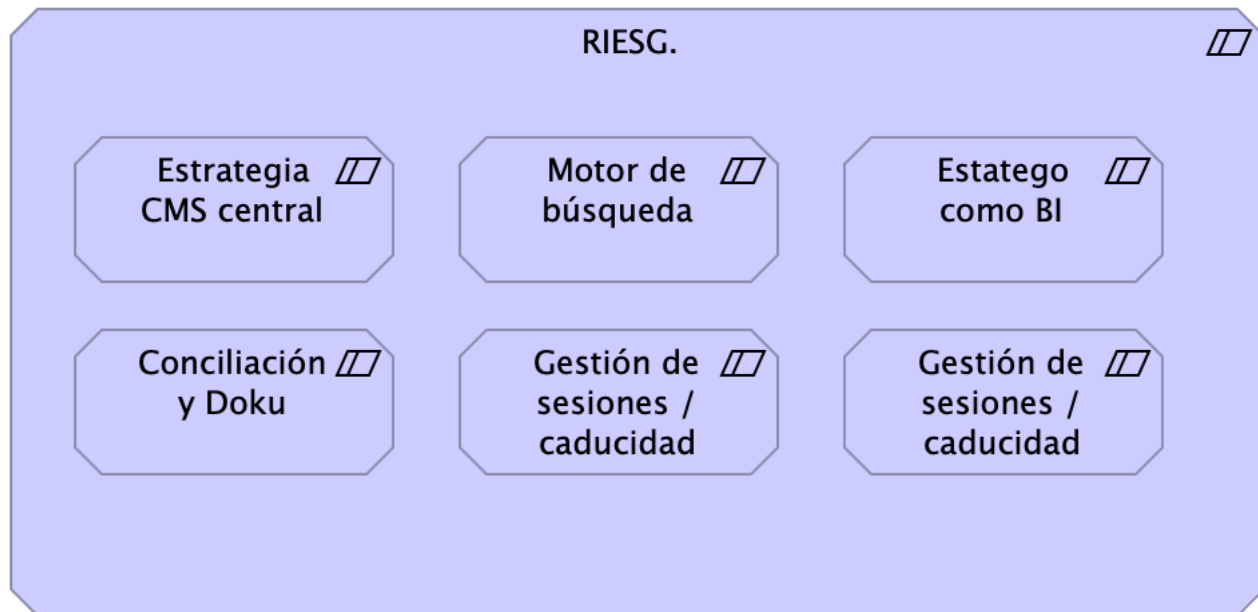
El portal es el conjunto de los elementos físicos y lógicos necesarios para la implementación de la granja de servidores de SharePoint Server 2019 para el portal de la PROCURADURIA.

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

Catálogo de Elementos

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

Riesgos.1



Catálogo de Elementos

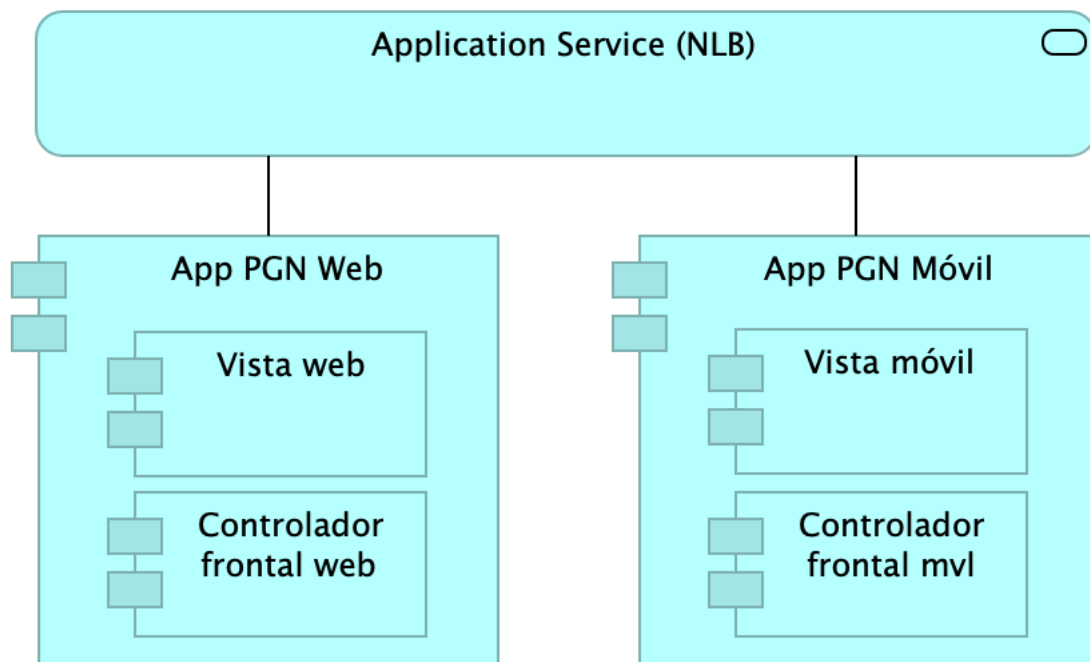
Name	Type	Description	Properties
Conciliación y Doku	constraint	Definir la ubicación de los componentes misionales de Conciliación Administrativa (SIU). Debe estar fuera de Doku.	
Estatego como BI	constraint	Definir la arquitectura de Estratego migrado: puede ser una solución de BI simple, o puede ser una aplicación web tradicional.	
Estrategia CMS central	constraint	Establecer desde el principio el gestor de contenidos compartido que los módulos del SUI migrados van a usar.	
Gestión de sesiones / caducidad	constraint	Establecer desde el principio el motor de búsqueda de conteidos compartido para los módulos del SUI migrados.	
Gestión de sesiones / caducidad	constraint	Definir la arquitectura de Estratego migrado: puede ser una solución de BI simple, o puede ser una aplicación web tradicional.	
Motor de búsqueda	constraint	Establecer desde el principio el motor de búsqueda de conteidos compartido para los módulos del SUI migrados.	
RIESG.	constraint	Asuntos de la Migración: <ul style="list-style-type: none">* Estrategia CMS central* Motor de búsqueda* Estatego como BI* Conciliación y Doku* Gestión de sesiones / caducidad	

Arquitectura Migración PGN SIU

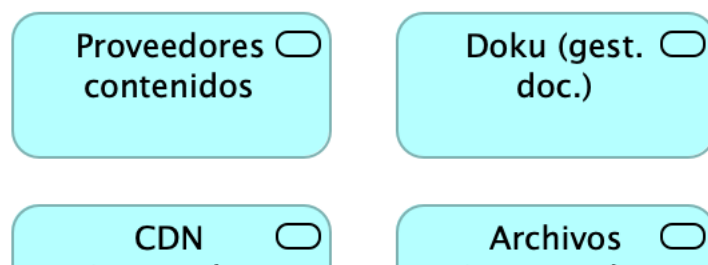
Migracion.1.SIU modulos

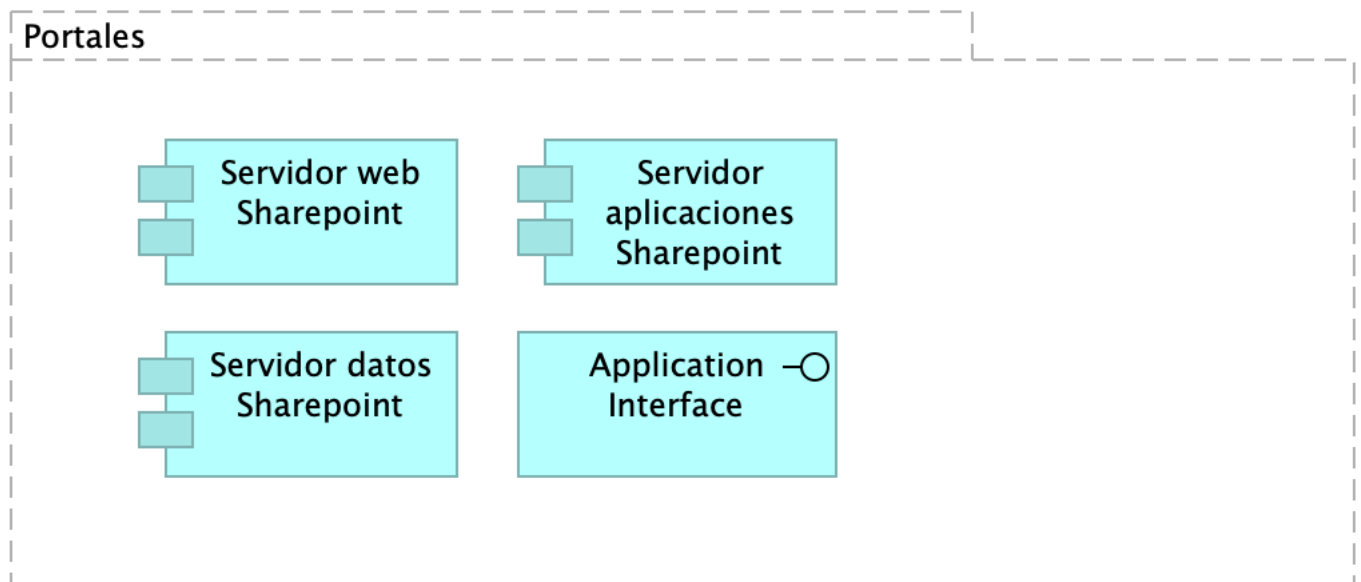
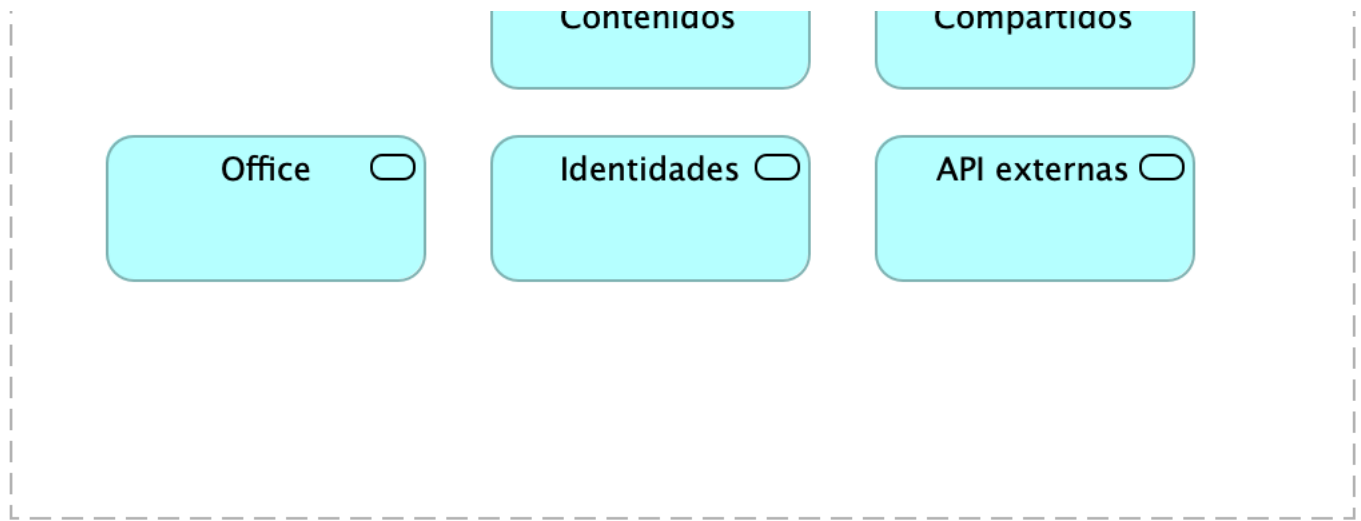
RQR. Funci

Presentación



Servicios de aplicación





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

Cuatro paquetes con tecnologías respectivas 1. Angular 11 (Web) 1. API Transaccional (Node Js) 1. API Config (C#) 1. Persistencia (SQL)

Catálogo de Elementos

Name	Type	Description	Properties
App	application-component		plataforma: node js
App PGN Móvil	application-component		
App PGN Web	application-component		plataforma: angular 11
Config	application-component		plataforma: cs
Controlador admin	application-component		plataforma: cs
Controlador frontal mvl	application-component		plataforma: js
Controlador frontal web	application-component		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
Servidor aplicaciones Sharepoint	application-component		
Servidor datos Sharepoint	application-component		

Name	Type	Description	Properties
Servidor web Sharepoint	application-component		
Transacciones	application-component		plataforma: sql
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		plataforma: angular 11
API externas	application-service		
Application Service (NLB)	application-service		plataforma: angular 11
Archivos Compartidos	application-service		
CDN Contenidos	application-service		
Doku (gest. doc.)	application-service		
Identidades	application-service		
Interfaz de datos 1	application-service		
Interfaz de datos 2	application-service		
Interfaz de datos 3	application-service		
Office	application-service		
Proveedores contenidos	application-service		
Mensaje: JSON	data-object		
Administración	grouping		
Almacenamiento	grouping		
PGN SIU	grouping		
Portales	grouping		
Presentación	grouping		
Servicios de aplicación	grouping		
RQR. Administrativos	requirement		
RQR. Funcionales	requirement		
RQR. Ingeniería	requirement		
RQR. Misionales	requirement		
RQR. Seguridad	requirement	<p>1. Las soluciones deben dar cumplimiento a las políticas institucionales del sistema de gestión de seguridad de la información establecidas por la entidad que busca garantizar la confidencialidad, integridad y disponibilidad de la información que se genera, procesa, almacena y/o transmite en los sistemas de Información de la Entidad.</p> <p>1. Las soluciones de automatización de procesos a implementar deben permitir la Gestión de Seguridad de Usuarios, grupos de usuarios y asignación de Roles y perfiles de usuarios, permitiendo asociar las acciones disponibles en la solución con respecto a roles de usuario, permitiendo parametrizar las funcionalidades que cada actor puede usar en la solución.</p> <p>1. Un usuario puede estar asociado a uno o más roles, de tal manera que los menús de navegación de la solución se muestran o despliegan dependiendo de las acciones asociadas a cada rol de usuario, permitiendo así que cuando el usuario es autenticado correctamente, la solución verifica los roles que tiene activos para otorgarle únicamente las acciones autorizadas.</p> <p>1. El diseño de la solución debe definir los criterios necesarios para asegurar la trazabilidad y auditoría sobre las acciones de creación, actualización, modificación o borrado de los componentes de información, de tal manera que la solución debe permitirle al administrador de la solución parametrizar las tablas y eventos que pueden auditarse.</p> <p>1. Las soluciones deben tener en cuenta mecanismos que aseguren el registro histórico para poder mantener la trazabilidad de las acciones realizadas por los usuarios, contemplando el registro de auditoría que contiene información de fecha y hora, identificación del registro, tabla afectada, descripción del evento, tipo</p>	

Name	Type	Description	Properties
		<p>de evento, usuario que realiza la acción, identificación de sesión y dirección IP del usuario que efectuó la transacción.</p> <p>1. La solución debe proveer una consulta que permita a un usuario con los privilegios asignados, consultar los registros de auditoría, aplicando criterios de filtro (usuario, máquina, rango de fechas y tipo de operación).</p> <p>1. Las soluciones deben integrarse con LDAP – (Lightweight Directory Access Protocol) para los procesos de inicio de sesión y autenticación. La solución debe soportar la integración Nativa con Active Directory de Microsoft. Para usuarios externos el mecanismo de autorización, autenticación y acceso será controlado a través del modelo de seguridad de la solución (no habrá autenticación para usuarios externos).</p> <p>1. Las soluciones deben cumplir con los lineamientos de seguridad relacionados a su utilización a través de redes públicas y privadas, garantizando la confidencialidad e integridad de la información y acceso a ella.</p> <p>1. Debe evidenciar que, a través de pruebas de vulnerabilidad, garantiza la seguridad de la información. Estas pruebas deben suministrar evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad.</p> <p>1. Debe incluir un mecanismo de cifrado de los datos que se transportan entre los diferentes componentes tecnológicos y los datos sensibles de la base de datos que representen un alto nivel de confidencialidad.</p> <p>1. A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio).</p> <p>1. Debe contemplar el cumplimiento de la normatividad vigente en cuanto a protección de datos personales y debe permitir el manejo de excepciones.</p> <p>1. Para los casos que aplique se debe permitir el manejo de certificados y/o firmas digitales en los documentos que así se definan para efectos de aprobación y digitalización.</p> <p>1. Debe contemplar las prácticas de desarrollo seguro de aplicaciones y/o implementación segura de productos, para su naturaleza Web based.</p> <p>1. Debe funcionar sobre protocolo SSL (certificados internos de la entidad cuando los sistemas de información sean internas y certificados validos públicamente cuando los sistemas de información estén expuestas a internet).</p> <p>1. Debe entregar un procedimiento para el respaldo de la información de acuerdo con las necesidades de la entidad.</p> <p>1. Debe incluir uso de criptografía para transacciones y/o campos sensibles según lo indiquen las normas vigentes y las necesidades específicas del negocio de acuerdo como lo determine la entidad.</p> <p>1. Debe contemplar un modelo de datos que garantice base de datos única para evitar que se pueda presentar duplicidad de información.</p> <p>1. En la información confidencial solo puede ser consultada por los perfiles autorizados e igualmente restringir documentos de consulta según los privilegios o permisos asociados.</p> <p>1. A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio).</p> <p>1. Debe cerrar las transacciones luego de máximo 10 minutos de inactividad.</p> <p>1. Debe incluir controles de bloqueo de cuenta después de un máximo de 5 intentos erróneos a fin de evitar ataques de fuerza bruta.</p> <p>1. Debe evidenciar el resultado positivo frente a pruebas de ethical hacking, análisis de vulnerabilidades, carga, estrés y desempeño antes de la puesta en operación de acuerdo con los lineamientos de la entidad.</p> <p>1. Debe cumplir con todos los</p>	

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

Generated on: Wed Aug 30 2023 16:12:51 GMT-0500 (COT)

Requerimientos de Administración

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

Requerimientos de Seguridad

- Las soluciones deben dar cumplimiento a las políticas institucionales del sistema de gestión de seguridad de la información establecidas por la entidad que busca garantizar la confidencialidad, integridad y disponibilidad de la información que se genera, procesa, almacena y/o transmite en los sistemas de Información de la Entidad.
- Las soluciones de automatización de procesos a implementar deben permitir la Gestión de Seguridad de Usuarios, grupos de usuarios y asignación de Roles y perfiles de usuarios, permitiendo asociar las acciones disponibles en la solución con respecto a roles de usuario, permitiendo parametrizar las funcionalidades que cada actor puede usar en la solución.
- Un usuario puede estar asociado a uno o más roles, de tal manera que los menús de navegación de la solución se muestran o despliegan dependiendo de las acciones asociadas a cada rol de usuario, permitiendo así que cuando el usuario es autenticado correctamente, la solución verifica los roles que tiene activos para otorgarle únicamente las acciones autorizadas.
- El diseño de la solución debe definir los criterios necesarios para asegurar la trazabilidad y auditoría sobre las acciones de creación, actualización, modificación o borrado de los componentes de información, de tal manera que la solución debe permitirle al administrador de la solución parametrizar las tablas y eventos que pueden auditarse.
- Las soluciones deben tener en cuenta mecanismos que aseguren el registro histórico para poder mantener la trazabilidad de las acciones realizadas por los usuarios, contemplando el registro de auditoría que contiene información de fecha y hora, identificación del registro, tabla afectada, descripción del evento, tipo de evento, usuario que realiza la acción, identificación de sesión y dirección IP del usuario que efectuó la transacción.
- La solución debe proveer una consulta que permita a un usuario con los privilegios asignados, consultar los registros de auditoría, aplicando criterios de filtro (usuario, maquina, rango de fechas y tipo de operación).
- 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).
- 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.
- 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.
- 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.
- A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio).
- Debe contemplar el cumplimiento de la normatividad vigente en cuanto a protección de datos personales y debe permitir el manejo de excepciones.
- 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.
- Debe contemplar las prácticas de desarrollo seguro de aplicaciones y/o implementación segura de productos, para su naturaleza Web based.
- 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).
- Debe entregar un procedimiento para el respaldo de la información de acuerdo con las necesidades de la entidad.
- 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.
- Debe contemplar un modelo de datos que garantice base de datos única para evitar que se pueda presentar duplicidad de información.
- En la información confidencial solo puede ser consultada por los perfiles autorizados e igualmente restringir documentos de consulta según los privilegios o permisos asociados.
- A nivel de la base de datos debe poder definirse reglas de validación de integridad de datos (unicidad, referencial y negocio).
- Debe cerrar las transacciones luego de máximo 10 minutos de inactividad.
- Debe incluir controles de bloqueo de cuenta después de un máximo de 5 intentos erróneos a fin de evitar ataques de fuerza bruta.

23. Debe evidenciar el resultado positivo frente a pruebas de ethical hacking, análisis de vulnerabilidades, carga, estrés y desempeño antes de la puesta en operación de acuerdo con los lineamientos de la entidad.
24. Debe cumplir con todos los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la "Guía de desarrollo OWASP" y "OWAS Cheat Sheet".

“

Referencias

[1] [eservices3-22?] [eservices4-22?] [eservices5-23?] [eservices6-12?] [eservices7-23?] [bptrends07?]

1. **Softgic. Proyecto de mejoramiento SIU de PGN. Fase i**
Softgic, PGN
(2022-06) <https://hwong23.github.io/fna-devdoc-f1/v/6497aef0f15c3591f0728e4c42cb2c26c13b43aa/>