# Arquitectura de Software: Infraestructura

* [Diagrama de Infraestructura de TI](#diagrama-de-infraestructura-de-ti)
  + [Migracion.3. Infraestructura](#migracion.3.-infraestructura)
  + [Lineabase.1a.SUI Componentes. Infraestrcutura](#X3f1f1b70ddb407784104160acaf60ebb6bc9d2d)
  + [Lineabase.0.SUI Aplicación. Física](#lineabase.0.sui-aplicación.-física)
  + [Seguridad.2. Lineabase.0.SUI Aplicación](#seguridad.2.-lineabase.0.sui-aplicación)
  + [Migracion.6. Migración de datos](#migracion.6.-migración-de-datos)
* [Documento sobre especificaciones técnicas de infraestructura TI](#X51db734b0c6c45519e8763ed857e3b1bb3c993c)
  + [Lineabase.0.SUI Aplicación. Física](#lineabase.0.sui-aplicación.-física)

# Diagrama de Infraestructura de TI

## Migracion.3. Infraestructura

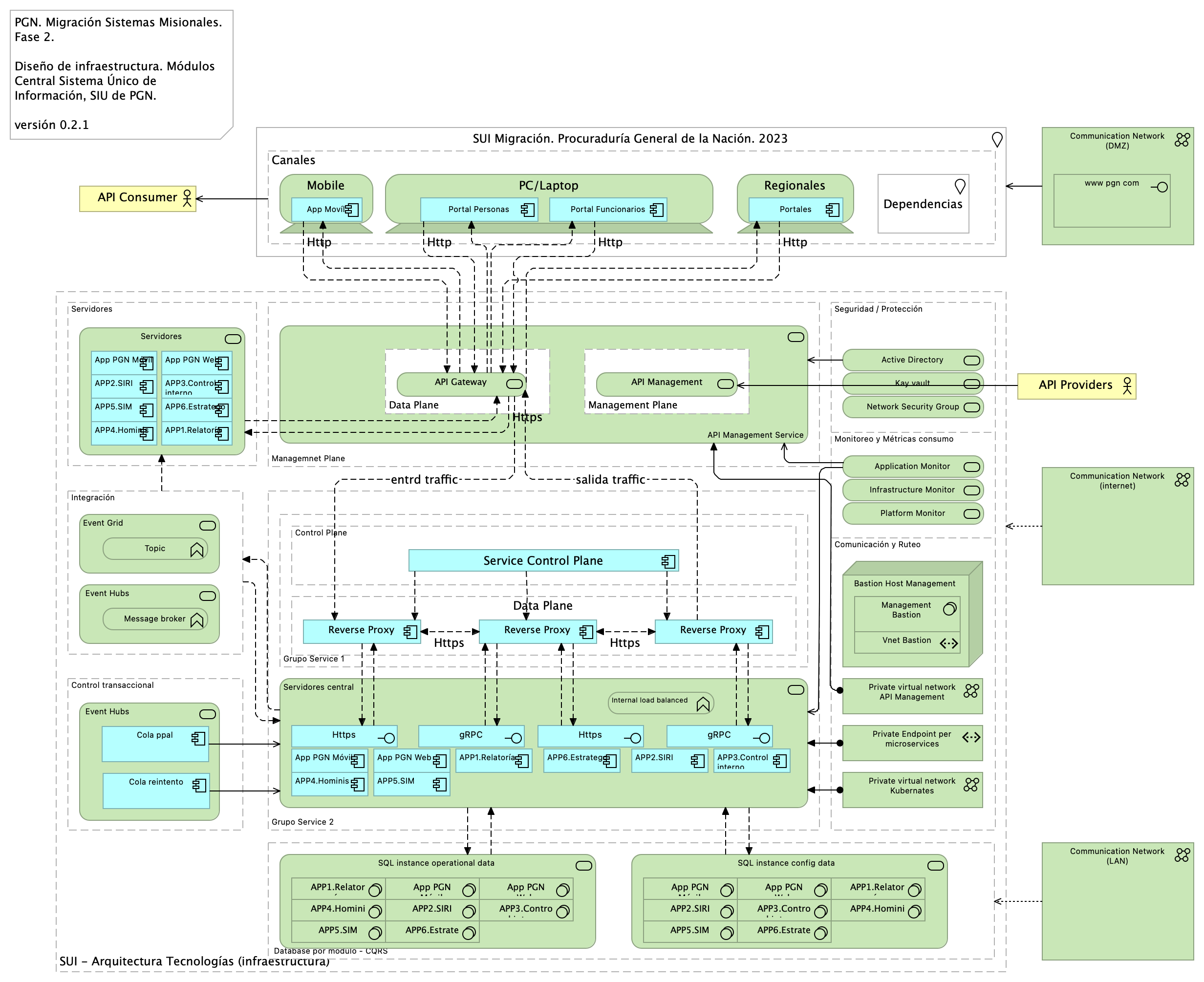


Figure 1: Vista. Migracion.3. Infraestructura

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. |  |
| **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. |  |
| **APP6.Estratego** | application-component | Módulo central SUI migrado. Módulo independiente y asignado a un dominio particular de la PGN: Estratego. |  |
| **App Movíl** | 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 Kubernates** | communication-network |  |  |
| **Mobile** | device |  |  |
| **PC/Laptop** | device |  |  |
| **Regionales** | device |  |  |
| \*\* Database por módulo - CQRS\*\* | grouping |  |  |
| **Canales** | grouping |  |  |
| **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 |  |  |
| **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. Infraestrcutura

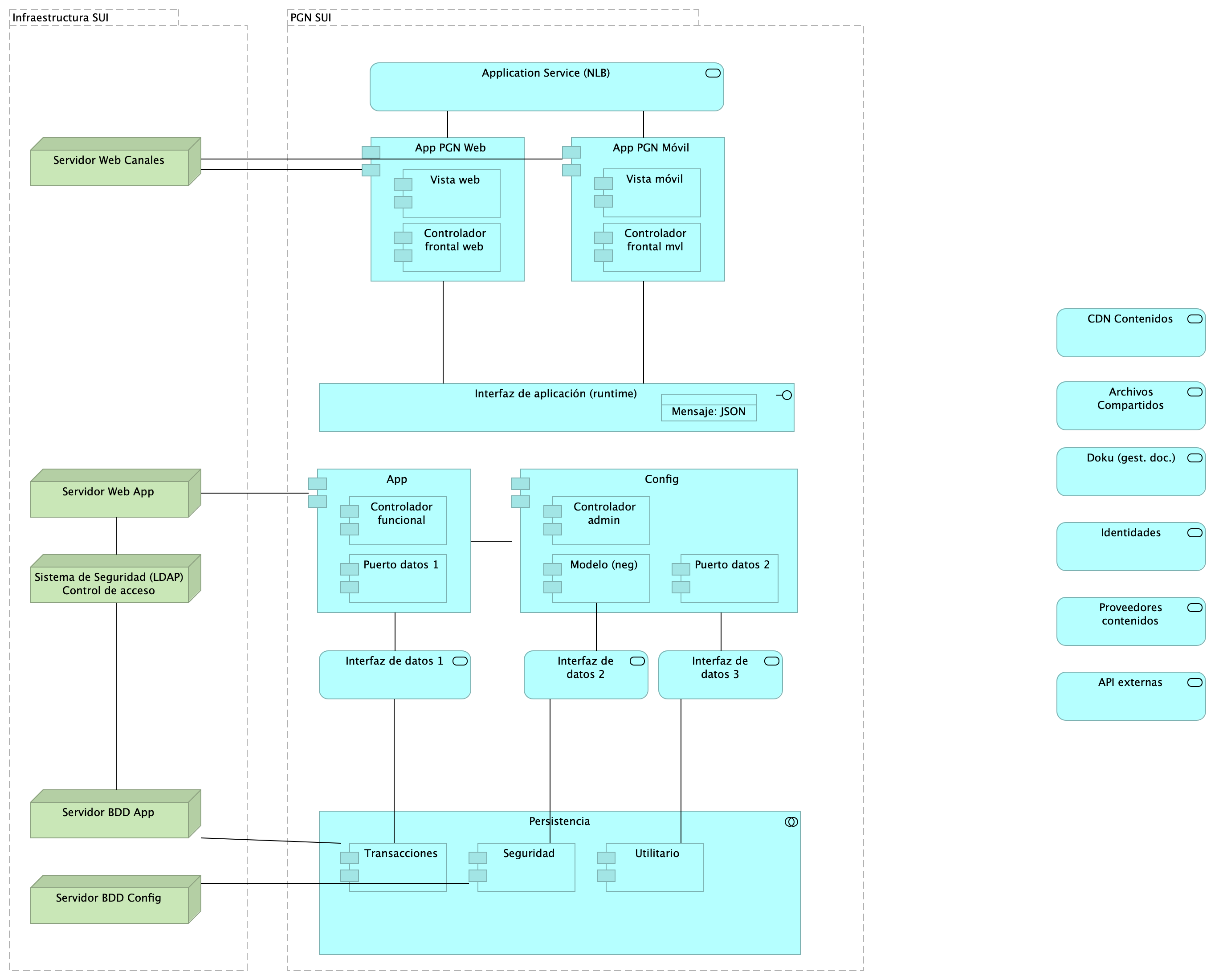


Figure 2: Vista. Lineabase.1a.SUI Componentes. Infraestrcutura

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



Figure 3: 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 |
| **App PGN Web** | application-component |  | *plataforma:* angular 11*brecha:* 100 |
| **Config** | application-component |  | *plataforma:* cs |
| **Punto acceso público** | application-interface | URL tipo CHTTP |  |
| **Application Service (NLB)** | application-service |  | *plataforma:* angular 11*brecha:* 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 |  |  |

## Seguridad.2. Lineabase.0.SUI Aplicación



Figure 4: 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 Identifiación 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 Segurida de la Información Confidencialidad e integridad, asimismo reducir los riesgos de la información mediante la ayuda de Técnicas Criptograficas.

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

Se propone integrar certificados SSL, que permite cifrar la información confidencial a fin de que solo los autorizados puedan tener acceso a ella, y 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 recopila:

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

### Catálogo de Elementos

| Nombre | Tipo | Descripción | Prop. |
| --- | --- | --- | --- |
| **Application Collaboration** | application-collaboration |  |  |
| **Application Collaboration** | application-collaboration |  |  |
| **App** | application-component |  | *plataforma:* node Js*brecha:* 100 |
| **App PGN Móvil** | application-component |  | *plantilla:* element-md-bold*brecha:* 100 |
| **App PGN Web** | application-component |  | *plataforma:* angular 11*brecha:* 100 |
| **Config** | application-component |  | *plataforma:* cs |
| **Punto acceso público** | application-interface | URL tipo CHTTP |  |
| **Application Service (NLB)** | application-service |  | *plataforma:* angular 11*brecha:* 100 |
| **Interfaz de datos 1** | application-service |  |  |
| **Interfaz de datos 2** | application-service |  |  |
| **Autenticación** | business-object |  |  |
| **Autorización** | business-object |  |  |
| **Cifrado de Datos en tránsito** | business-object |  |  |
| **Cifrado de datos en tránsito** | business-object |  |  |
| **Communication Network (DMZ)** | communication-network |  |  |
| **Communication Network (LAN)** | communication-network |  |  |
| **Communication Network (internet)** | communication-network |  |  |
| **Balanceador** | node |  |  |
| **Firewall BDD** | node |  | *brecha:* 100 |
| **Network Firewall/WAF** | node |  | *brecha:* 100 |
| **Servidor BDD App** | node | Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz. Discos SO C: 126 GB, Backup E: 511 GB, SQL Data F: 510 GB, SQL Log G: 510 GB, TempDB G: 63.6 GB. |  |
| **Servidor BDD Config** | node | Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 Ghz. Discos SO C: 80 GB, Backup E: 250 GB, SQL Data F: 250 GB, SQL Log G: 250 GB, TempDB G: 30 GB. |  |
| **Servidor Web App** | node | Windows Server 2019 Standard o Datacenter x64. Nombre físico. IP LAN. IP Pública. Windows Server 2019 Standard or Datacenter x64. RAM 8 GB. CPU 64 Bits. 4 Cores de 2 Ghz. Discos SO C: 126 GB. SO D: 16 GB. |  |
| **Servidor Web Canales** | node | Windows Server 2019 Standard o Datacenter x64. Nombre físico. IP LAN. IP Pública. Windows Server 2019 Standard or Datacenter x64. RAM 8 GB. CPU 64 Bits. 4 Cores de 2 Ghz. Discos SO C: 126 GB. SO D: 16 GB. |  |
| **Sistema de Seguridad (LDAP) 1** | node | Sistema de Seguridad (LDAP) 1. Control de acceso internet, La autenticación podrá estar integrada con el directorio activo, a partir de la generación de codigo para ek ingreso con 2FA, que podrá generar un código la plataforma de correo corporativo, el cual solicitará el codigo de autenticacion y una vez ingreado podrá redirigir al sitio. | *brecha:* 100 |
| **Sistema de Seguridad (LDAP) 2** | node | Sistema de Seguridad (LDAP) 2. Control de acceso internet, La solución se podra integrar con el directorio activo, a partir de la generación del 2FA, que podrá generar un codigo por desde la plataforma de office 365, el cual solicitará el codigo de autenticacion y una vez ingreado podrá acceder al sitio. | *brecha:* 100 |
| **www pgn com** | technology-interface |  |  |

## Migracion.6. Migración de datos



Figure 5: 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 arquitecura 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. |
| --- | --- | --- | --- |
| **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. |  |
| **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. |  |
| **Servidor BDD App 2** | node | Sistema Operativo Windows Server 2019 Standard o Datacenter x64. RAM 8 GB. CPU 64 Bits, 4 Cores > 2 GhzDiscos 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 GhzDiscos 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 GhzDiscos 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



Figure 6: 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 |
| **App PGN Web** | application-component |  | *plataforma:* angular 11*brecha:* 100 |
| **Config** | application-component |  | *plataforma:* cs |
| **Punto acceso público** | application-interface | URL tipo CHTTP |  |
| **Application Service (NLB)** | application-service |  | *plataforma:* angular 11*brecha:* 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 |  |  |

Generated on: Tue Dec 05 2023 13:46:58 GMT-0500 (COT)