## Lineabase.0.SUI applicación



Figure 1: Diagram: Lineabase.0.SUI applicación

Procuraduría General de la Nación, proyecto Migración SUI, 2023, Fase II. Línea base del sistema único de información (SUI en adelante) de la PGN. Presentación de componentes de software originales implementados en la Fase I del presente proyecto.

## Representación Arquitectónica

Con una arquitectura orientada a servicios SUI recopila:

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

### Catálogo de Elementos

| Name | Type | Description | Properties |
| --- | --- | --- | --- |
| **Application Collaboration** | application-collaboration |  |  |
| **Application Collaboration** | application-collaboration |  |  |
| **App** | application-component |  | *plataforma:* node Js*brecha:* 100 |
| **App PGN Móvil** | application-component | A partir de los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la “Guía de desarrollo OWASP” y “OWAS Cheat Sheet, se realizaran pruebas de seguridad a partir del analisis de vulnerabilidades, y pruebas de Ethikal Hacking. Protección de datos personales, Los sistemas de información que recogen, procesan y almacenan información de los derechos de las personas se deben almacenar de forma adecuada, la información que pueda ser vulnerada puede generar obliaciones legales y éticas con respecto a la perdida de informacion confidencial por parte de ciudadanos del pais. La informacion contenida en las bases de datos debe tener los mecanismos de cifrado que en otros apartados se han mencionado. La legislación que hay que tener como referencia, ley 1581 de 2012. Decreto 1377 de 2013La metodologia empleada tendrá las siguientes fases: • FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como:o Recopilación de dominios/IPs/puertos/servicioso Recopilación de metadatoso Uso de Google Dorks.• ANÁLSIS DE VULNERABILIDADES: Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades. • EXPLOTACIÓN: • Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo: o Inyección de códigoo Inclusión de ficheros locales o remotoso Evasión de autenticacióno Carencia de controles de autorizacióno Ejecución de comandos en el lado del servidoro Ataques tipo Cross Site Request Forgeryo Control de erroreso Gestión de sesioneso Fugas de informacióno Secuestros de sesióno Comprobación de las condiciones para realizar una denegación de servicio. • POST EXPLOTACIÓN:En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adiciones con el objetivo de comprobar la criticidad de esta.No URL IP1. https://runtimetest.lappiz.io/#/auth/login/PGN\_Lappiz135.181.185.207 | *plantilla:* element-md-bold*brecha:* 100 |
| **App PGN Web** | application-component | A partir de los lineamientos de desarrollo seguro establecidos en The OWASP Foundation recomendados en la “Guía de desarrollo OWASP” y “OWAS Cheat Sheet, se realizaran pruebas de seguridad a partir del analisis de vulnerabilidades, y pruebas de Ethical Hacking. Los resultados permitirán identificar los requisitos de seguridad que los sistemas de informacion o servicios web deberán cumplir.La metodologia empleada tendrá las siguientes fases: • FASE DE RECONOCIMIENTO: Se recolectará toda la información posible, usando diferentes técnicas como:o Recopilación de dominios/IPs/puertos/servicioso Recopilación de metadatoso Uso de Google Dorks.• ANÁLSIS DE VULNERABILIDADES: Se analizará la información recopilada en la fase anterior y se realizará el descubrimiento de las vulnerabilidades. • EXPLOTACIÓN: • Se realizarán todas aquellas acciones que puedan comprometer al sistema auditado, las pruebas a implementar pueden ser de ataques tipo: o Inyección de códigoo Inclusión de ficheros locales o remotoso Evasión de autenticacióno Carencia de controles de autorizacióno Ejecución de comandos en el lado del servidoro Ataques tipo Cross Site Request Forgeryo Control de erroreso Gestión de sesioneso Fugas de informacióno Secuestros de sesióno Comprobación de las condiciones para realizar una denegación de servicio. • POST EXPLOTACIÓN:En caso de encontrarse una vulnerabilidad que permita realizar otras acciones en el sistema auditado o en su entorno, se realizarán controles adiciones con el objetivo de comprobar la criticidad de esta.No URL IP1. https://runtimetest.lappiz.io/#/auth/login/PGN\_Lappiz135.181.185.207El Login deberá evidenciar el control de errores, al momento de realizar la validación deberá mensaje de error para el caso que se autentique con credenciales erradas. | *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 |  |  |