## Riesgos.1. Migración funcional



Figure 1: Diagram: Riesgos.1. Migración funcional

Riesgos de la migración funcional:

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

### Acciones de Mitigación

1. Informar a la PGN de las implicaciones junto con alternativas para la implementación de la acción de aprovechamiento: diseño del SCM central (sharepoint). La PGN debe decidir si o no a la acción propuesta.
2. Informar a la PGN de las implicaciones junto con alternativas para la implementación de la acción de aprovechamiento: diseño del motor de búsqueda compartido (sharepoint). La PGN debe decidir si o no a la acción propuesta.
3. Informar a la PGN de las implicaciones junto con alternativas para la implementación de la acción de manejo del riesgo: diseño de solución de inteligencia de negocio (Power BI). La PGN debe decidir si o no a la acción propuesta.
4. Informar a la PGN de las implicaciones junto con alternativas para la implementación de la acción de manejo del riesgo: ubicar la lógica, los flujos, y los datos misionales dentro del SIU. La PGN debe decidir si o no a la acción propuesta.
5. Informar a la PGN de las implicaciones junto con alternativas para la implementación de la acción de manejo del riesgo: facilitar la administración de seguridad en un solo lugar (distinto de localizarla en las aplicaciones web). La PGN debe decidir si o no a la acción propuesta.

### Catálogo de Elementos

| Name | Type | Description | Properties |
| --- | --- | --- | --- |
| **RSG1. Estrategia CMS central** | constraint | Establecer desde el principio el gestor de contenidos compartido que los módulos del SUI migrados van a usar. |  |
| **RSG10. Validación decisiones de arquitectura** | constraint | Discutir la arquitectura de referencia de SUI Migración PGN. La arquitectura de referencia SUI informa de todas las fortalezas y consideraciones estructurales y de sistema, como extensibilidad, rendimiento y seguridad, que regirán a todos los módulos del SUI migrado. |  |
| **RSG11. Estrategias de Migración de datos** | constraint | Discutir el alcance y los recursos para la correcta migración de datos incluídas en contrato 078, Migración Funcional SIU en atención al numeral 5.6 del anexo técnico del proyecto. | 5.6 MIGRACIÓN DE DATOS |
| **RSG12. Arquitectura de almancenamiento y distribución de datos SIU** | constraint | Definir la opción de organización y distribución de los almacenes de datos del SIU. opc1. Dispositivo físico/virtual (nodo, servidor, y esquema de base de datos) único, central, a todos los módulos del SIU.opc2. Dispositivos virtuales autónomos por dominio de negocio: rlatoría, inventario, información estratégica, intercomunicados. |  |
| **RSG13. Sistema de autenticación híbrido** | constraint | Definir la estrategia de autenticación del SIU migrado (aplicable a todos los módulos del SIU migrado).opc1. Híbrida: integrado, directorio empresarial (LDAP), y servicios de autenticación de confianza: Office 365 de PGN.opc2. Servicio de autenticación de confianza: Office 365 de PGN. |  |
| **RSG2. Motor de búsqueda compartido** | constraint | Establecer desde el principio el motor de búsqueda de conteidos compartido para los módulos del SUI migrados. |  |
| **RSG3. Estatego como BI** | constraint | Definir la arquitectura de Estratego migrado: puede ser una solución de BI simple, o puede ser una aplicación web tradicional. |  |
| **RSG4. Conciliación y gestión documental (Doku)** | constraint | Definir la ubicación de los componentes misionales de Conciliación Administrativa (SIU). Debe estar fuera de Doku. |  |
| **RSG5. Gestión de sesiones / caducidad** | constraint | Establecer desde el principio el motor de búsqueda de conteidos compartido para los módulos del SUI migrados. |  |
| **RSG6. Componentes de negocio** | constraint | Incluir el esfuerzo de creación de componentes estrcturales y comunes a los módulos del SUI migrado requeridos por la arquitectura de referencia SUI. Algunos componentes requeridos son:\* Administración de autorizaciones (integrado con el directorio PGN)\* Motor de flujos de trabajo para diseño y organización del trabajo (Conciliación)\* Componente de ruteo de documentos (Relatoría) |  |
| **RSG7. Asignación de roles y permisos de Acceso** | constraint | RSG7. Asignación de roles y permisos de AccesoLos riesgos de autenticación como el Single Sign On (SSO), permite que si las credenciales de usuario se ven comprometidas, pueden dar permiso a un atacante acceder a todos o la mayoría de recursos y aplicaciones en la red. Se ha propuesto controlar los accesos a partir de la documentación que identifica la metodología de clasificación y gestión de usuarios roles y procesos de autenticación, a partir del control de acceso basado en roles RBAC (Identidades y autenticación), que permite tener una reacción más oportuna para controlar los accesos a diferentes módulos de los diferentes sistemas de Información. Los inicios de sesión de los usuarios asociados a cuenta de dominio de Active Directory deben tener en cuenta la asignación de roles de ingreso al servidor o roles de ingreso al motor de bases de datos. Las cuentas de usuario no deben ser creadas de administrador local (administrador), es una puerta de entrada para los ataques de fuerza bruta. |  |
| **RSG8. Intentos de accesos no autorizados** | constraint | RSG8. Intentos de accesos no autorizadosLos intentos no autorizados son una de las técnicas más comunes utilizadas en la actualidad, los diferentes tipos de amenazas de intrusiones SQL Injections, Denegaciones de Servicios, riesgos de Ransomware, Ingeniería social, malware y otras amenazas, permite que se proponga implementación de soluciones de Seguridad perimetral a partir de la implementación de WAF para controlar las peticiones externas y evaluación de vulnerabilidades y escaneo para conocer puertos abiertos y establecer medidas. |  |
| **RSG9. Alteración de datos negocio** | constraint | RSG9. Alteración de datos almacenados en Base de Datos.Se deberán asignar usuarios para la conexión de cada base de datos.Se debe proporcionar seguridad a nivel de filas y columnas (ofuscamiento) para proteger los datos confidenciales en el nivel de columnas y filas RLS ((seguridad de nivel de fila). Algunos de los métodos y características que se deben tener en cuenta a implementar es a partir del Alway encrypted, para cifrar los datos que se encuentran almacenados. |  |
| **Riesgos Técnicos Migración Funcional SUI (078)** | constraint | Conjunto de riesgos técnicos y arquitectura. Proyecto Migración SUI 2023, PGN. |  |