



Defensa Jurídica
del Estado

**PLAN ESTRATÉGICO DE
TECNOLOGÍAS DE LA
INFORMACIÓN Y LAS
COMUNICACIONES – PETI
2024 - 2027**

**UNIDAD ADMINISTRATIVA ESPECIAL
AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO
ENERO DE 2024**

TABLA DE CONTENIDO

1.	INTRODUCCIÓN	3
2.	OBJETIVO	3
3.	ALCANCE	3
4.	DEFINICIONES Y ABREVIATURAS	4
5.	NORMATIVIDAD	5
6.	DESARROLLO	5
6.1	ESTRATEGIA DE TI	5
	SERVICIOS DE TI	7
	GOBIERNO DE TI.....	8
	GESTIÓN DE INFORMACIÓN.....	11
	SISTEMAS DE INFORMACIÓN	15
	INFRAESTRUCTURA TI	19
	SEGURIDAD	21
6.2	DISTRIBUCIÓN PRESUPUESTAL	21
6.3	MAPA DE RUTA 2024 – 2027	22
7.	RIESGOS	23
8.	INDICADORES	23
9.	CRONOGRAMA.....	23

1. INTRODUCCIÓN

El Plan Estratégico de Tecnologías de la Información (PETI) para el período 2024-2027 de la Agencia Nacional de Defensa Jurídica del Estado ofrece una visión futura y ambiciosa que servirá como brújula para los próximos años. A través de la identificación de brechas críticas, se han formulado estrategias específicas, dando forma a iniciativas concretas que no solo abordarán las necesidades inmediatas de la agencia, sino que también estarán alineadas con sus objetivos estratégicos a largo plazo.

Este documento condensa la esencia de un enfoque proactivo y orientado hacia el futuro para la gestión de tecnologías de la información, reconociendo la importancia crucial de mantenerse a la vanguardia en un entorno dinámico y desafiante. Las estrategias delineadas no solo buscan cerrar las brechas existentes, sino que también procuran potenciar las capacidades de la agencia, garantizando así su capacidad para enfrentar los desafíos emergentes con agilidad y eficacia.

Exploraremos los elementos clave que componen el PETI 2024-2027, desde su análisis situacional hasta las iniciativas concretas que se proponen. Este plan estratégico representa no solo una hoja de ruta para la transformación tecnológica, sino también un compromiso con la excelencia en la prestación de los servicios de la agencia respaldados por un ecosistema tecnológico robusto y avanzado.

2. OBJETIVO

El objetivo general de este documento es presentar el Plan Estratégico de Tecnologías de la Información (PETI) de la Agencia Nacional de Defensa Jurídica del Estado para el año 2024

Los objetivos específicos son:

- Definir una estrategia de Tecnologías de la Información (TI) que esté alineada con el Plan Estratégico de la Agencia y que responda a los requerimientos y necesidades de negocio.
- Formular un mapa de ruta de proyectos de tecnología que de manera táctica implementen la estrategia definida.

3. ALCANCE

El PETI aborda de manera integral los dominios de arquitectura de negocio, sistemas de información, tecnología, información y seguridad. En este enfoque,

se realiza un análisis detallado para determinar una estrategia tecnológica respaldada por un mapa de proyectos. Este mapa se configura con el objetivo de satisfacer las necesidades e intenciones del negocio, alineándose de manera precisa con el cumplimiento de los objetivos y metas estratégicas de la Agencia.

4. DEFINICIONES Y ABREVIATURAS

Las siguientes son las definiciones y abreviaturas que se manejarán a lo largo del documento.

Abreviaturas y siglas	Significado
AGN	Archivo General de la Nación
MIPG	Modelo integrado de planeación y gestión
SGDEA	Sistema de Gestión de Documentos Electrónicos de Archivo
AE	Arquitectura Empresarial.
AI (Artificial Intelligence)	Combinación de algoritmos planteados con el propósito de crear máquinas que presenten las mismas capacidades que el ser humano.
Aprendizaje automático (Machine Learning)	Conjunto de tecnologías y algoritmos usados para el aprendizaje supervisado y no supervisado guiados por las lecciones encontradas en la información existente.
Backup	Copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.
BD	Base de datos.
BPM (Business Process Management)	Conjunto de metodologías y tecnologías, cuyo objetivo es mejorar el desempeño y la optimización de los procesos de una organización.
BRM (Business Rules Management)	Sistema de software utilizado para definir, implementar, ejecutar, monitorear y mantener la lógica de decisión que utilizan los sistemas dentro de una organización.
CONPES	Consejo Nacional de Política Económica y Social.
Data lake	Repositorio de almacenamiento de datos de una organización sin una estructura predefinida.
DDJI	Dirección de Defensa Jurídica Internacional.
DDJN	Dirección de Defensa Jurídica Nacional.
DGI	Dirección de Gestión de Información.
DPE	Dirección de Políticas y Estrategias para la Defensa Jurídica.
eKOGUI	Sistema Único de Gestión e Información de la Actividad Litigiosa.
ETL (Extract, Transform and Load)	Proceso que permite a las organizaciones mover datos desde múltiples fuentes, reformatearlos y limpiarlos, y cargarlos en otro sistema o almacén de datos.
Framework	Marco de trabajo o marco metodológico.
Metamodelo	Es un grafo que contiene cuatro tipos de elementos, Entidad, atributo, asociación y restricción.

MSPI	Modelo de Seguridad y Privacidad de la Información.
OCR (Optical Character Recognition)	Proceso dirigido a la digitalización de textos, los cuales identifican automáticamente a partir de una imagen símbolos o caracteres que pertenecen a un determinado alfabeto, para luego almacenarlos en forma de datos.
RAP (Robot Process Automation)	Conjunto de tecnologías que integran la ejecución robotizada de acciones en la automatización de procesos de negocio.
SG	Secretaría General.
SDJ	Sistema de Defensa Jurídica.
SGDEA	Sistema de Gestión de Documentos Electrónicos de Archivo.
SIDH	Sistema Interamericano de Derechos Humanos
TI	Tecnologías de la información.

Tabla 1. Definiciones y abreviaturas

5. NORMATIVIDAD

El Plan Estratégico de TI 2024-2027, refleja y se encuentra acorde con todas las políticas y lineamientos de Gobierno establecido para las Entidades del sector público, rigiéndose también en un contexto normativo definido por el entorno del sector justicia y del derecho y del sector de las TIC, así como las normas y directrices establecidas por la ANDJE en los procesos y procedimientos formalizados en DARUMA.

6. DESARROLLO

Producto de sesiones estratégicas y de una comprensión integral de la Agencia, este DOFA refleja las Debilidades, Oportunidades, Fortalezas y Amenazas. Con el fin de maximizar las fortalezas, abordando las debilidades, capitalizando oportunidades y enfrentando las amenazas de manera proactiva. A continuación, se deja un alto nivel del DOFA.

6.1 ESTRATEGIA DE TI

La estrategia de TI se ha definido para reflejar la intención de la entidad en relación con su ecosistema de TI y cómo evolucionará para satisfacer las necesidades y generar valor estratégico.

Misión de TI

Ser un aliado estratégico para la Agencia Nacional de Defensa Jurídica del Estado mediante la generación de valor con TICs, alineado al cumplimiento del modelo de intención, con la ejecución de planes, programas, proyectos y capacidades

orientadas al liderazgo y gestión de sus soluciones tecnológicas y la optimización de los recursos TIC con calidad, oportuno y generando valor.

Visión de TI

Para el año 2027, la Oficina Asesora de Sistemas y Tecnologías de la Agencia Nacional de Defensa jurídica será ampliamente reconocida por su capacidad para enfrentar los desafíos de transformación digital, apropiar las tecnologías de última generación y promover la innovación dentro de la entidad por medio impulsada por tecnología.

Objetivos estratégicos de TI

Se proponen los siguientes objetivos estratégicos, con metas definidas, alineados con la visión y evolución de la Agencia en cuanto a su ecosistema de TI.

Objetivo estratégico de TI	Meta
Implementar tecnológicas alineadas al soporte de los procesos y servicios de la Agencia.	Soportar el 100% de los procesos de la Agencia con tecnologías de la información para el 2027.
Definir los servicios de TI y optimizar su entrega para garantizar eficiencia operativa, satisfacción del cliente y alineación con las necesidades del negocio.	Garantizar cumplimiento del plan de continuidad de negocio con respecto a RTO y RPO de servicios críticos.
	Realizar encuestas de satisfacción a los funcionarios y contratistas de la Agencia.
Mantener una infraestructura tecnológica y soluciones de TI actualizada para adoptar soluciones modernas que impulsen la agilidad, la innovación y la escalabilidad, mejorando así la eficiencia de la Agencia.	Migrar la infraestructura tecnológica de Ekogui a una arquitectura de nube híbrida en un 100% para el 2027.
Mantener un Modelo de Gestión y Gobierno TIC, como instrumento habilitador tanto de la estrategia de la Entidad como de los procesos de la Agencia Nacional de Defensa Jurídica del Estado	Implementar el 100% del Modelo de Gobierno y Gestión de TI para 2027.
Contribuir a la Transformación Digital de la Entidad, desde el dominio de tecnología, tomando los elementos de la Política de Gobierno Digital del Estado como marco de uso, apropiación y cumplimiento	Cumplir con los indicadores de cada plan estratégico de acuerdo con las metas propuestas.
Promover la explotación de los datos e información para la toma de decisiones y la generación de conocimiento en materia de Defensa Jurídica del Estado	Cumplir con la implementación del 100% el plan de la estrategia y gobernanza de la infraestructura de datos para la Agencia en el 2027.

Garantizar la protección integral de los activos de información de la organización mediante la implementación de un robusto modelo de seguridad y privacidad de la información, mitigando riesgos y fortaleciendo la postura de seguridad contra amenazas internas y externas.	Asegurar el cumplimiento del 100% del modelo de seguridad y privacidad de la información de la Entidad.
--	---

Tabla 2. Objetivos estratégicos de TI de la Agencia – estado objetivo

SERVICIOS DE TI

La Oficina Asesora de Sistemas y Tecnologías de Información de la Agencia ajusta su portafolio de servicios de TI para ofrecerlo a nivel interno y externo de la Agencia y alineándose a la consecución de los objetivos estratégicos de TI.

Los servicios en su situación deseada son:

Servicio
Soporte y mantenimiento a sistemas de información y herramientas de TI
Acceso a la red interna de la Agencia (intranet)
Gestionar proveedores de TI
Acceso a internet
Servicios de comunicaciones de TI para la Entidad
Gestión de infraestructura centro de datos y servidores
Acceso a la red interna por VPN
Gestión de contingencia y continuidad de los servicios de TI
Gestión de la seguridad de la infraestructura
Desarrollo y mantenimiento de sistemas de información de la Agencia
Definición e implementación de proyectos de TI
Capacitación técnica de sistemas de información
Soporte técnico mediante la mesa de servicios
Servicio de antivirus
Gestión de equipos de cómputo
Servicios de Instalación de software en Equipos de computo
Configuración de ambientes de los sistemas de información
Administración de bases de datos
Pruebas de vulnerabilidades
Gestión de identidades
Servicio DNS
Servicio de Virtualización de servidores
Aseguramiento de la calidad del software
Adquisición de licencias de software
Servicio de interoperabilidad
Plataforma de mesa de servicio
Gestión de backups

Tabla 3. Lista de servicios TI – estado objetivo

GOBIERNO DE TI

Políticas y estándares para la gestión de la gobernabilidad de TI

Las políticas de TI de la Agencia son definidas y adoptadas conforme a los lineamientos del Marco de Referencia de Arquitectura Empresarial de MINTIC, acogiendo las políticas establecidas por el Gobierno Nacional y define aquellas específicas que le permiten la toma de decisiones para gobernar y gestionar las TI. La Agencia, deberá complementar sus políticas y alineación a estándares como se muestra a continuación.

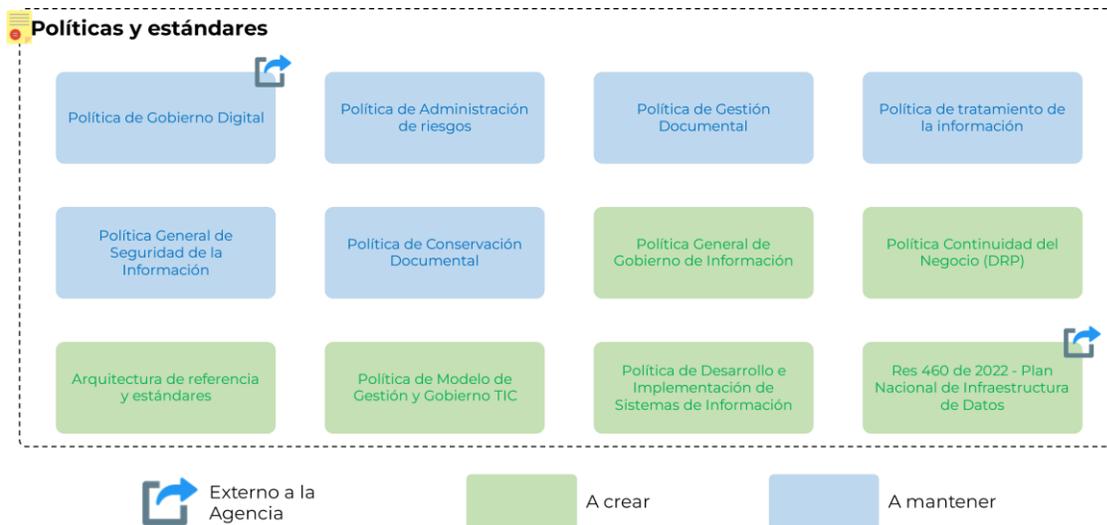


Ilustración 1. Políticas y estándares – estado objetivo

Gestión y Supervisión del Presupuesto de Inversiones y gastos de Operación de las TIC

La gestión y supervisión del presupuesto de inversiones y gastos de operación de las TIC financiera de TI de la Agencia no supone cambios, es decir, se seguirá soportando bajo el Plan Anual de Adquisiciones (PAA) de la Entidad en la que se identifican las inversiones que realiza la Agencia para la adquisición de recursos, servicios y consultorías de TI.

Procesos de Gestión de TI

La cadena de valor de TI se fortalece por medio del ajuste y alineación de los procedimientos de TI con marcos de referencia de gobierno y gestión de TI como COBIT, con el fin de adoptar mejores prácticas que facilite la alineación de TI con el negocio para generar valor, así como su constante evolución.

Estructura organizacional de TI

Para garantizar la ejecución de los procedimientos propuestos y alineación con las políticas y estándares definidos dentro del ejercicio, la OASTI debe fortalecerse con la inclusión de roles y responsabilidades definidas que permitan el gobierno y gestión de las TIC dentro de la Entidad.

Categoría	Rol
Jefatura	Jefe OASTI
Gobierno y gestión de TI	Contractual y Financiero
	Planes Estratégicos
	Gobierno de TI y datos
	Arquitecto Empresarial
	Uso y Apropiación
Gestión de servicios de TI e infraestructura	Gestor de mesa de servicio
	Gestor de infraestructura híbrida
	Gestor de activos de TI
Sistemas de Información	Desarrollador
	Pruebas
	DBA
	Arquitecto solución de los sistemas de información
	Líder técnico de los sistemas de información
Sistema de gestión de seguridad de la información	Seguridad
Contratos y consultorías	Fábricas de desarrollo de software
	Proveedores de servicios de TI

Tabla 4. Estructura organizacional – estado objetivo

Esquema de toma de decisiones

La toma de decisiones en lo relacionado con las TIC se fortalece por medio de 4 instancias de tomas de decisiones en los que participa o lidera la OASTI, los cuales se realizan de manera periódica y tienen objetivos puntuales. A continuación, la Ilustración 2. muestra las instancias de tomas de decisiones propuestas.

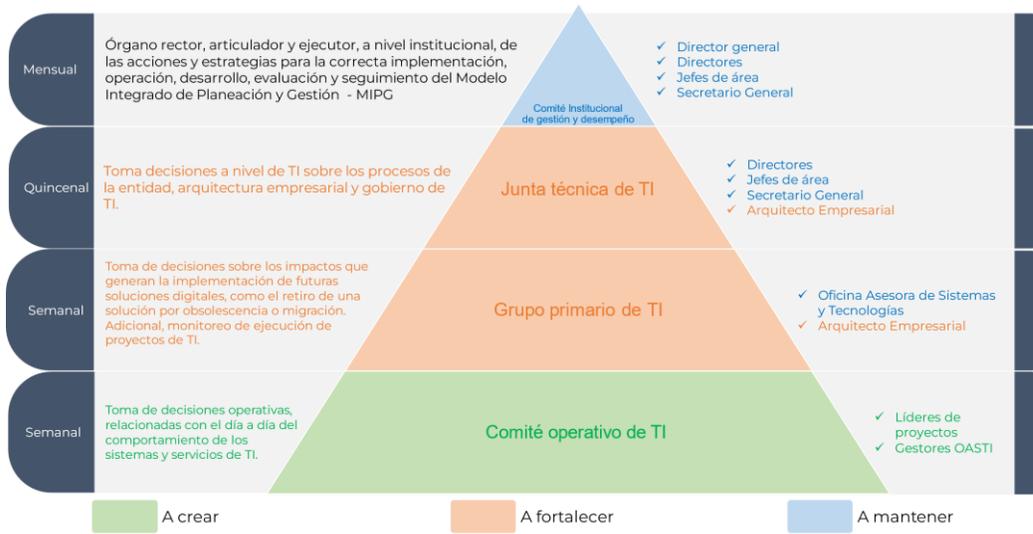


Ilustración 2. Instancias de tomas de decisiones situación deseada

Gobierno de arquitectura

La OASTI lidera la definición y ejecución de la estrategia digital de la Entidad, asegurando que la arquitectura empresarial se alinee con los objetivos estratégicos institucionales como los de TI de la Agencia. Por lo tanto, se define un gobierno de arquitectura el cual se debe implementar como situación objetivo.

El modelo de gobierno de arquitectura requiere la participación de los arquitectos empresariales y de solución, con el fin de que garantizar que las soluciones tecnológicas sean definidas y detalladas conforme a estándares y a la arquitectura de referencia de la Entidad. A continuación, la Ilustración 3. representa el modelo de arquitectura de la Agencia.



Ilustración 3. Modelo de gobierno de arquitectura – estado objetivo

Gestión de Proyectos

El Ministerio de las Tecnologías de la Información y las Comunicaciones (MINTIC) define un modelo para la gestión de los proyectos de TI (MGPTI) que establecen lineamientos para la administración de los proyectos e implementando mejores prácticas de gestión. Por lo tanto, se espera que en la situación objetivo se fortalezca la gestión de proyectos de TI adoptando este modelo con el fin de garantizar la ejecución.

GESTIÓN DE INFORMACIÓN

La Agencia tiene como objetivo principal abordar las definiciones relacionadas con la Estrategia y Gobernanza de la Infraestructura de Datos, la Interoperabilidad de la Infraestructura de Datos y la Seguridad y Privacidad de Datos para el año 2027. Estas definiciones estarán alineadas con el Plan Nacional de Infraestructura de Datos (PNID).

Principios y Marco de Entendimiento del PNID adoptados por la ANDJE:

1. **Calidad de los Datos:** La agencia se compromete a gestionar conjuntos de datos, especialmente los datos maestros, para garantizar su integridad y utilidad.
2. **Fácil Búsqueda, Accesibilidad, Interoperabilidad y Reutilización:** Los datos de la Agencia seguirán los principios FAIR para garantizar su fácil búsqueda, accesibilidad, interoperabilidad y reutilización, respetando principios legales.
3. **Seguridad y Protección de los Datos:** La agencia garantizará la seguridad y protección de los datos personales en todas las fases del ciclo de vida.

4. **Privacidad por Diseño y por Defecto:** Se implementarán medidas preventivas desde las etapas iniciales para proteger la privacidad y confidencialidad de la información.
5. **Confianza Pública y Gestión Ética de los Datos:** La agencia asegurará que sus datos generen confianza en el ecosistema del PNID.
6. **Estandarización e Interoperabilidad:** La agencia se adherirá a definiciones de estandarización, APIs y arquitecturas distribuidas para su incorporación eficiente en el PNID.
7. **Sectorización Estratégica:** Se aplicarán normativas y estándares para mitigar riesgos en la incorporación de la agencia con el PNID.

Respecto a la adopción del Marco de Entendimiento de la Infraestructura de Datos:

1. **Estrategia y Gobernanza de la Infraestructura de Datos:** La agencia implementará estrategias específicas para la gestión eficiente de datos maestros y transaccionales, fortaleciendo capacidades analíticas y toma de decisiones basadas en datos.
2. **Interoperabilidad de la Infraestructura de Datos:** Se consolidarán estándares comunes para facilitar la reutilización e intercambio de datos, priorizando la implementación de protocolos de intercambio de datos.
3. **Seguridad y Privacidad de Datos:** La agencia asegurará la integridad y confidencialidad mediante infraestructura técnica avanzada, manuales de seguridad detallados y sistemas de autorización y autenticación sólidos.
4. **Uso de la Nube:** Se migrará hacia la nube para aprovechar esquemas de seguridad avanzados, actualizaciones regulares y soluciones de respaldo, alineándose con los estándares del PNID.

Arquitectura de Información

La Agencia está trabajando en un análisis detallado para establecer un sólido modelo de gobierno de datos y definir la arquitectura de información.

La OASTI jugará un papel clave al orientar y respaldar la implementación de servicios tecnológicos para alcanzar los objetivos de la agencia. Proporcionará asesoría estratégica y apoyo táctico, priorizando la alineación de servicios tecnológicos con los objetivos específicos de gobierno de datos.

La OASTI se esforzará por ofrecer recursos de vanguardia, destacando la adopción de componentes en la nube para optimizar la eficiencia operativa, garantizar la seguridad y accesibilidad de datos, y promover la escalabilidad.

En colaboración con equipos internos, la OASTI identificará soluciones tecnológicas adecuadas, considerando seguridad, integridad e interoperabilidad. Se enfocará en tres enfoques clave para establecer un entorno de gobierno sólido y sostenible:

La OASTI se centrará en tres enfoques cruciales:

1. **Generación de Valor:** La arquitectura se enfocará en transformar datos en información significativa para respaldar decisiones y alcanzar objetivos estratégicos.
2. **Empaquetado de Servicios de Información:** La información se conceptualizará en servicios específicos, adaptados a las necesidades de diversos grupos de interés para facilitar su comprensión y uso.
3. **Disponibilidad y Calidad:** Se garantizará la disponibilidad constante de información, priorizando la calidad mediante prácticas y estándares que fortalezcan la integridad y confiabilidad de los datos. La adopción de tecnologías en la nube permitirá una optimización efectiva de recursos.

Servicios de Intercambio de datos

La Agencia está implementando acciones para el registro de procesos judiciales de alta litigiosidad, optimizando la interoperabilidad de binarios y datos mediante servicios web. Estos servicios se alinean con el modelo X-ROAD, un estándar reconocido para el intercambio seguro de datos.

El enfoque estratégico busca mejorar la interacción de los usuarios con los servicios judiciales, reduciendo la carga operativa a través de la interoperabilidad de binarios y datos. La adopción del modelo X-ROAD garantiza una base sólida para el intercambio seguro de información, fortaleciendo la eficiencia operativa y la integridad de los datos en el ámbito judicial.

La Agencia tiene como objetivo alcanzar una cobertura del 100% al 2027 con el modelo X-ROAD, sin exponer servicios directos que eludan este estándar. Se contempla la implementación de un API Manager con la migración de eKOGUI a la nube, ofreciendo beneficios clave como capacidades de autenticación y autorización, transformación de datos, gestión de límites y cuotas, monitoreo detallado y facilitación de la migración a la nube. Estas medidas mejorarán la eficiencia y seguridad de las operaciones internas de la Agencia.

Gestión de la calidad y seguridad de la información

La Agencia integrará una estrategia integral de información en su modelo de gestión de datos. Esto incluirá políticas rigurosas de calidad y seguridad para garantizar la integridad, confidencialidad y disponibilidad de los datos. La gestión

de calidad se enfocará en estándares precisos, procedimientos y procesos, mientras que la seguridad de la información se abordará con medidas avanzadas, como autenticación robusta y cifrado de datos. Esta estrategia demuestra el compromiso de la agencia con la excelencia en la gestión de datos, facilitando decisiones informadas y la creación de valor a lo largo de su evolución.

Análisis y aprovechamiento de la información

La Agencia busca optimizar la eficiencia operativa y mejorar sus servicios mediante el análisis de tendencias y correlaciones, anticipando cambios clave derivados de acciones de madurez en la gestión de datos, el Plan Nacional de Infraestructura de Datos, la migración a la nube de eKogui y el fortalecimiento de las arquitecturas tecnológicas.

La agencia ha destacado en el desarrollo de soluciones analíticas, pero la concentración de componentes internos plantea desafíos de escalabilidad y costos operativos. La migración a la nube ofrece oportunidades para mejorar la escalabilidad y flexibilidad, con una transición planificada y progresiva.

Además, la agencia contempla la adopción de servicios en la nube para optimizar procesos analíticos, aprovechando modelos de lenguaje avanzados, aprendizaje automático como servicio (MLaaS), plataformas de análisis y procesamiento de datos, servicios de orquestación, base de datos multimodelo, plataforma de integración como servicio (IPaaS), computación sin servidor, búsqueda administrada, gestión de identidades y accesos, y servicios cognitivos.

En el análisis de transición hacia la nube, se propone la evaluación de servicios como MLFlow, servicios cognitivos de visión, y la migración de flujos ETL/ELT a modelos PaaS e iPaaS.

Finalmente, se presentan dos casos específicos: "Evolución eKogui - capacidades de datos y analítica" y "Búsqueda avanzada - IA Generativa", que reflejan la estrategia de la agencia para mejorar la interacción y eficiencia mediante servicios analíticos avanzados y la adopción de tecnologías en la nube.

Desarrollo de capacidades para el uso de la información

La Agencia tiene como objetivo el desarrollo de capacidades para potenciar el uso gerencial y estratégico de la información. Esto se logrará a través de la transformación estratégica de eKogui y la implementación de iniciativas específicas.

EKogui: Transformación Estratégica en la Defensa Jurídica:

- Mejora integral de la plataforma eKogui para brindar un apoyo más eficiente a los abogados del Estado.
- Automatización y optimización de procesos legales, reduciendo el tiempo invertido en tareas rutinarias.
- Adaptación continua a cambios normativos y control de litigiosidad y desempeño de usuarios.
- Consolidación de eKogui como gestor de casos con alertas personalizadas, trazabilidad de procesos, herramientas analíticas avanzadas, descarga de documentos simplificada y módulos específicos.

Vista 360 de los Usuarios en la Comunidad Jurídica del Conocimiento (CJC):

- Fortalecimiento de la CJC para mejorar la calidad del litigio público.
- Ofrece información jurídica actualizada, herramientas de gestión de procesos judiciales y programas de formación.
- Implementación de una vista 360 de los usuarios mediante CRM Dynamics 365 para personalizar servicios, contenidos y mejorar la comunicación y atención al cliente.

Casos Focales para la Implementación Progresiva del PNID:

- Alineación estratégica con el Plan Nacional de Infraestructura de Datos (PNID).
- Iniciativa segmentada y focalizada para implementar gradualmente los requisitos del PNID.
- Generación de casos de negocio específicos para abordar las necesidades de la agencia y sus entidades asociadas, asegurando flexibilidad y adaptabilidad a cambios gubernamentales.

SISTEMAS DE INFORMACIÓN

La Agencia busca fortalecer su papel estratégico y orquestador de la defensa jurídica a través de cambios en sus sistemas de información. El enfoque se centra en mejorar la eficiencia de los procesos relacionados con la entidad. Las estrategias transformacionales incluyen:

1. Fortalecimiento de Canales Digitales:

- Mejorar el acceso a servicios y la interacción mediante múltiples canales.
- Adoptar estándares definidos en la Ley 2052 de 2020.
- Fortalecer la interacción con la comunidad jurídica, defensores y entidades nacionales y territoriales.

2. Balancear Aplicaciones para Labores Estratégicas:

- Priorizar el despliegue en la nube para garantizar disponibilidad, seguridad y una experiencia positiva para el usuario.
- Enfocar esfuerzos en labores estratégicas y de orquestación de defensa jurídica.

3. Control de Información a través de Sistemas de Información:

- Utilizar sistemas de información como puntos únicos de entrada y salida de información.
- Gobernar la información y gestionar controles de seguridad para reducir riesgos asociados a la manipulación de datos en hojas de cálculo y otros medios.

4. Optimización con Nuevas Capacidades Tecnológicas:

- Fortalecer capacidades con tecnologías como inteligencia artificial, aprendizaje de máquina y automatización de procesos.
- Integrar nuevas funcionalidades para mejorar la eficiencia y el rendimiento de las aplicaciones.

5. Interoperabilidad e Integración entre Aplicaciones:

- Implementar la interoperabilidad para permitir la integración con otras aplicaciones y tecnologías.
- Facilitar el flujo de información y reducir tareas manuales en la Agencia.

Se ejecutarán acciones específicas sobre los sistemas de información existentes, como reemplazar Orfeo con la implementación de SGD Mercurio, evolucionar LegisOffice como parte de la transformación de eKogui, y centralizar la gestión de casos en el CRM MS Dynamics 365. Estas acciones buscan mejorar la consistencia, accesibilidad y seguridad de la información, respaldando así la posición estratégica de la ANDJE en la defensa jurídica del Estado.

Mapa de Integraciones objetivo de los Sistemas de Información

La Agencia fortalecerá el intercambio de información entre sus sistemas de información. El enfoque incluye la creación de un Gestor de Interoperabilidad y soluciones de integración que permitirán una comunicación más eficiente entre los componentes del ecosistema tecnológico de la agencia y actores externos. Las integraciones clave son las siguientes:

1. Gestor de Interoperabilidad:

- Agrega servicios de integración e interoperabilidad.
- Utiliza un API Manager para definir un catálogo de servicios y un API Gateway para controlar el tráfico.
- Expone servicios según contratos definidos por la Plataforma de Interoperabilidad del Estado Colombiano.

2. Aplicaciones Exponiendo Capacidades de Integración:

- **Gestor de Casos eKogui:** Envía reportes diarios de operación, información sobre procesos, conciliaciones y pagos asociados a casos judiciales.
- **Biblioteca Digital:** Reporta información de sentencias asociadas al estado de casos jurídicos y entidades de conocimiento jurídico.
- **SGD Mercurio:** Recopila documentos de soporte a procesos jurídicos.

3. Aplicaciones Consumiendo Capacidades de Servicios:

- **Gestor de Casos eKogui:** Asocia soportes documentales gestionados por el SGD Mercurio para cada proceso generado.
- **Biblioteca Digital:** Recopila información de procesos gestionados por eKogui para asociación con sentencias judiciales.
- **CRM:** Asocia información obtenida mediante capacidades de servicio para la consulta de procesos jurídicos y partes involucradas.

4. Plataforma de Interoperabilidad del Estado Colombiano:

- Permite el reporte de pagos asociados a procesos judiciales, consultas de procesos de la Rama Judicial y Entidades Públicas de Alta Litigiosidad.
- Facilita el reporte de conciliación de procesos judiciales ante la Procuraduría General de la Nación.

Arquitectura de Referencia

La Agencia establecerá las Arquitecturas de Referencia para guiar estratégicamente el desarrollo de soluciones y mejorar la eficiencia de intercambio de información. Se contemplarán los siguientes aspectos:

Principios de Intercambio de Información:

- Utilización de estándares como web service REST, web service SOAP, Socket, DBLink, etc.
- Componentes transversales de integración como ESB, Bróker, API Gateway.
- Componentes de seguridad para APIs expuestas hacia otras

organizaciones.

Seguridad:

- Garantía de confidencialidad con Gestor de Identidades, servidor LDAP, Soluciones Single Sign On, encriptación y enmascaramiento de datos.
- Solución transversal de log de transacciones para auditar acciones en sistemas.

Software y Service Selection:

- Potenciación del uso de la plataforma CRM y sus módulos.
- Reducción en el número de integraciones y archivos de usuario final susceptibles de automatización.
- Uso de tecnologías estándares como API REST FULL-JSON, colas de mensajes, SFTP o ETLs.

Principios de Incorporación Tecnológica:

- Preferencia por soluciones SaaS, PaaS, y IaaS como opciones nativas en la nube.
- Justificación necesaria para opciones On-premises.

Separación de Ambientes:

- Claridad y separación de ambientes de desarrollo, pruebas y producción para garantizar la integridad del sistema.
- Evitar desarrollo en ambientes personales y migrar a infraestructura como servicio para eKogui.

Ciclo de Vida de los Sistemas de Información

La Agencia fortalecerá el procedimiento de "Gestión del ciclo de vida de sistemas de información", alineado con metodologías ágiles y DevSecOps para asegurar la entrega continua de valor y el desarrollo eficiente de sistemas. El ciclo de vida de los sistemas de información comprende las siguientes fases y acciones de mejora:

Fases del ciclo de vida de SI	Acción de mejora (Actividades a incluir)
Levantamiento de necesidades de Sistemas de Información	Recopilar las necesidades de sistemas de información según requerimientos de áreas, Arquitectura de Referencia y mejoras.

	Incluir documentación de prácticas DevSecOps.
Análisis de requisitos funcionales y no funcionales	Documentación de prácticas de DevSecOps.
Diseño de la solución	Actividades formales y estructuradas de diseño de arquitectura de sistemas de información
Codificación del software	Documentación de prácticas de DevSecOps.
Aseguramiento de la calidad (pruebas)	Documentación de prácticas de DevSecOps.
Documentación del Sistema de Información	Documentación técnica de los sistemas de información e incluir documentación de prácticas de DevSecOps.
Mantenimiento de Sistemas de Información	Incluir el mantenimiento correctivo y preventivo a todos los sistemas de información
Despliegue en Producción	Documentación de prácticas de DevSecOps.

Tabla 5. Ciclo de vida de los SI - situación objetivo

Este enfoque integral propende por que los sistemas de información evolucionen eficientemente, cumplan con los requisitos y se alineen con las mejores prácticas de seguridad y desarrollo continuo.

Soporte de los Sistemas de Información

El procedimiento de solicitud de servicios de TI incluirá un mecanismo de escalamiento adecuado para dirigir los casos al nivel correspondiente. Este enfoque garantizará una respuesta efectiva y especializada a los distintos niveles de incidencias y contribuye a mantener la estabilidad y eficiencia de los sistemas de información de la Agencia. A continuación, se describe:

Actividad	Responsable
Soporte de aplicaciones nivel 1	Gestor de mesa de servicios
Soporte de aplicaciones nivel 2	Líder técnico de los sistemas de información
Soporte de aplicaciones nivel 3	Desarrollador DBA Proveedor de sistema de información

Tabla 6. Soporte de los SI - situación objetivo

INFRAESTRUCTURA TI

La Agencia busca desarrollar una estrategia de infraestructura de TI que garantice la disponibilidad y operación eficiente de sus servicios e implemente un modelo de servicios integral. El enfoque se basa en cuatro criterios clave: Arquitectura de Servicios Tecnológicos, Operación, Soporte y Gestión de Calidad y Seguridad de Servicios Tecnológicos.

A continuación, se describen los servicios de infraestructura a fortalecer o implementarse

Servicio de infraestructura	Acciones para desarrollar
Servicio de nube	<i>A evolucionar.</i> El objetivo es disponer de servicios que se utilizarán como funciones del Sistema para la Gestión de Casos eKogui
Servicio de Redes	<i>Mantener.</i> Los servicios de conectividad no se ven afectados por la migración de soluciones a la Nube
Servicio de seguridad	<i>A evolucionar.</i> Los servicios de acceso a funcionalidades y capacidades se migran a la solución de IDP en Nube. Por otro lado, las capacidades de control de tráfico serán manejadas bajo esquema híbrido; con aspectos involucrados en Nube Pública para el control de peticiones hacia eKogui.
Servicio de servidores	<i>Mantener</i>
Servicio de almacenamiento	<i>A reemplazar.</i> Al reemplazar el SGD Orfeo por SGD Mercurio, el servicio de almacenamiento se usará como plataforma asociada a la solución de Software como Servicio (PaaS) que provee el SGD futuro.
Servicio de telefonía	Mantener
Servicio de facilities	A evolucionar. Al realizarse iniciativas de migración de eKogui a Software como Servicio en Nube, se delega la disponibilidad de los servicios involucrados a la Infraestructura como Servicio dispuesta en Nube
Servicio de Periféricos	Mantener

Tabla 2. Servicios de Infraestructura de TI - situación objetivo

Adicionalmente, para llevar a cabo la administración efectiva de la capacidad de infraestructura tecnológica en la Agencia, se considerarán los siguientes aspectos clave:

Interoperabilidad: Establecer mecanismos tecnológicos para facilitar la interoperabilidad de sistemas de información, tanto internos como externos.

Seguridad y Privacidad: Implementar herramientas y controles definidos en el Modelo de Seguridad y Privacidad de la Información, abarcando componentes On-Premise y en la Nube.

Aprovechamiento de Capacidades en la Nube: Aprovechar capacidades contratadas a través de servicios de nube pública para habilitar elementos transversales de servicios tecnológicos, incluyendo:

- Transformación digital.

- Inteligencia de negocios.
- Analítica avanzada.
- Laboratorio de innovación con tecnologías disruptivas.
- Capacidades de procesamiento de cómputo como servicio.
- Publicación de portales en herramientas de gestión de contenido adquiridas como servicio.
- Inteligencia artificial para apoyar procesos de negocio.
- Contar con el soporte adecuado de capacidad de cómputo en la nube pública para el diseño e implementación del Plan de Recuperación de Desastres.
- Optimizar y extender los licenciamientos de las herramientas tecnológicas utilizadas, considerando la actualización sobre la modalidad de servicio en la nube.

SEGURIDAD

La Agencia tiene como prioridad establecer sólidos lineamientos tecnológicos y garantizar el cumplimiento de estándares y buenas prácticas en seguridad y privacidad de la información. Para fortalecer estos aspectos, se proponen las siguientes acciones:

- Definir claramente el rol de oficial de tratamiento de datos personales, en conformidad con la política de tratamiento de datos personales de la entidad.
- Establecer un protocolo completo de seguridad de la información que incluya la protección de activos, controles criptográficos, control de acceso físico, defensa contra códigos maliciosos, aseguramiento de servicios en red, gestión de la continuidad, ingreso seguro a sistemas, gestión de usuarios e identificación y clasificación de activos.
- Actualización de Controles de Seguridad:
- Actualizar los controles de seguridad implementados por la Agencia conforme a los estándares de la norma ISO 27001:2022.
- Evaluación del Modelo de Seguridad y Privacidad de la Información:
- Ejecutar una evaluación exhaustiva del Modelo de Seguridad y Privacidad de la Información, teniendo en cuenta los controles de seguridad definidos por la ISO 27001:2022.

Estas acciones se centran en fortalecer la protección de los activos de información de la entidad, garantizando una gestión efectiva de la seguridad y privacidad de los datos, y asegurando la alineación con los estándares y controles de seguridad más recientes.

6.2 DISTRIBUCIÓN PRESUPUESTAL

De acuerdo con la proyección PAA las siguientes adquisiciones hacen parte de los controles para fortalecer el sistema de seguridad y privacidad de la información.

7. RIESGOS

CLASIFICACIÓN DEL RIESGO	DESCRIPCIÓN DEL RIESGO	CAUSAS	CONSECUENCIAS	CONTROLES
Estratégico	Incumplimiento de metas propuestas para los planes de acción institucional de TI.	Insuficiente de asignación de tiempos y recursos Disminución de presupuesto	Incumplimientos legales y llamados de atención	Planificación y entrega del PAA a Financiera

8. INDICADORES

(A) Porcentaje de implementación del PETI.

9. CRONOGRAMA

RESULTADO ESPERADO	PESO (%)	RESULTADOS / ENTREGABLES INTERMEDIOS	PESO (%)	RESPONSABLE	EJECUCIÓN	
					Fecha Inicio	Fecha Final
Evolución eKogui como gestor de casos jurídicos	11%	Arquitectura de solución del sistema de información, diseñada para que sea cloud native.	50%	OASTI/DGI	15/03/2024	31/07/2024
		Nuevas funcionalidades sobre el sistema desarrolladas	50%	OASTI/DGI	1/08/2024	31/12/2024
Migración cloud eKogui	11%	Arquitectura de eKOGUI refactorizada para que sea cloud native	33%	OASTI	15/03/2024	31/07/2024
		Solución en la nube híbrida de la probada	33%	OASTI	1/08/2024	31/10/2024
		Solución en la nube híbrida desplegada.	34%	OASTI	1/11/2024	31/12/2024
Estrategia e implementación modelo de gobierno de datos y preparación hacia el PNID	11%	Modelo de gobierno de datos aplicado en los casos de uso seleccionados.	50%	OASTI	1/05/2024	31/12/2024
		Parámetros del PNID para los casos de uso aplicados	50%	OASTI	1/05/2024	31/12/2024
Implementación estrategia de uso y apropiación	11%	Estrategia de uso y apropiación aplicada en cada iniciativa de TI realizada	100%	OASTI	15/01/2024	31/12/2024
Potencialización e innovación a través de la adecuada apropiación del CRM	11%	CRM promovido necesidades. Incremento de transacciones	50%	OASTI	1/03/2024	31/07/2024
		Herramientas de Mantis y GLPI migradas	50%	OASTI	1/08/2024	31/12/2024

Implementación del SGDEA	11%	Sistema de Gestión de Documentos Electrónicos de Archivo implementado	50%	OASTI /GD	15/01/2024	31/07/2024
		2 flujos adicionales implementados en el SGDEA	50%	OASTI /GD	1/08/2024	31/10/2024
Fortalecimiento de Seguridad	11%	Rol de oficial de seguridad creado	25%	OASTI	15/01/2024	30/04/2024
		Controles de Seguridad de TI con definiciones ISO27001 - 2022 actualizados según cronograma	25%	OASTI	1/03/2024	31/12/2024
		Proceso de Gestión de Seguridad de la Información definido y publicado	25%	OASTI	1/02/2024	30/04/2024
		Plan de continuidad de negocio BCP implementado	25%	OASTI	1/03/2024	31/12/2024
Implementación modelo de gobierno de arquitectura	11%	Modelo de arquitectura empresarial de la Agencia guiado por el Marco de Referencia de Arquitectura Empresarial del Estado Colombiano (MRAE) definido y socializado	33%	OASTI/OAP	1/03/2024	30/06/2024
		Dominios de arquitectura Empresarial socializado	33%	OASTI/OAP	1/07/2024	30/11/2024
		Referencias y estándares del MRAE definidos y socializados.	34%	OASTI/OAP	1/07/2024	31/12/2024
Implementación modelo de gestión y gobierno de TI	12%	Estructura organizacional, roles, responsabilidades definidos e incluidos en Procedimientos	33%	OASTI	1/03/2024	30/06/2024
		Procesos, prácticas y estándares documentados y publicados, instancias de tomas de decisiones) que permitan fortalecer en la Agencia el modelo de gobierno y gestión de TI	33%	OASTI	1/07/2024	30/09/2024
		Instancias de tomas de decisiones incluida en Procedimiento, publicado	34%	OASTI	1/10/2024	30/12/2024

Elaboró	Revisó	Aprobó
Liliana Barbosa Carrillo Gestor T1-15	Oswaldo Useche Acevedo Jefe Oficina	Comité Institucional de Gestión y Desempeño - CIGD