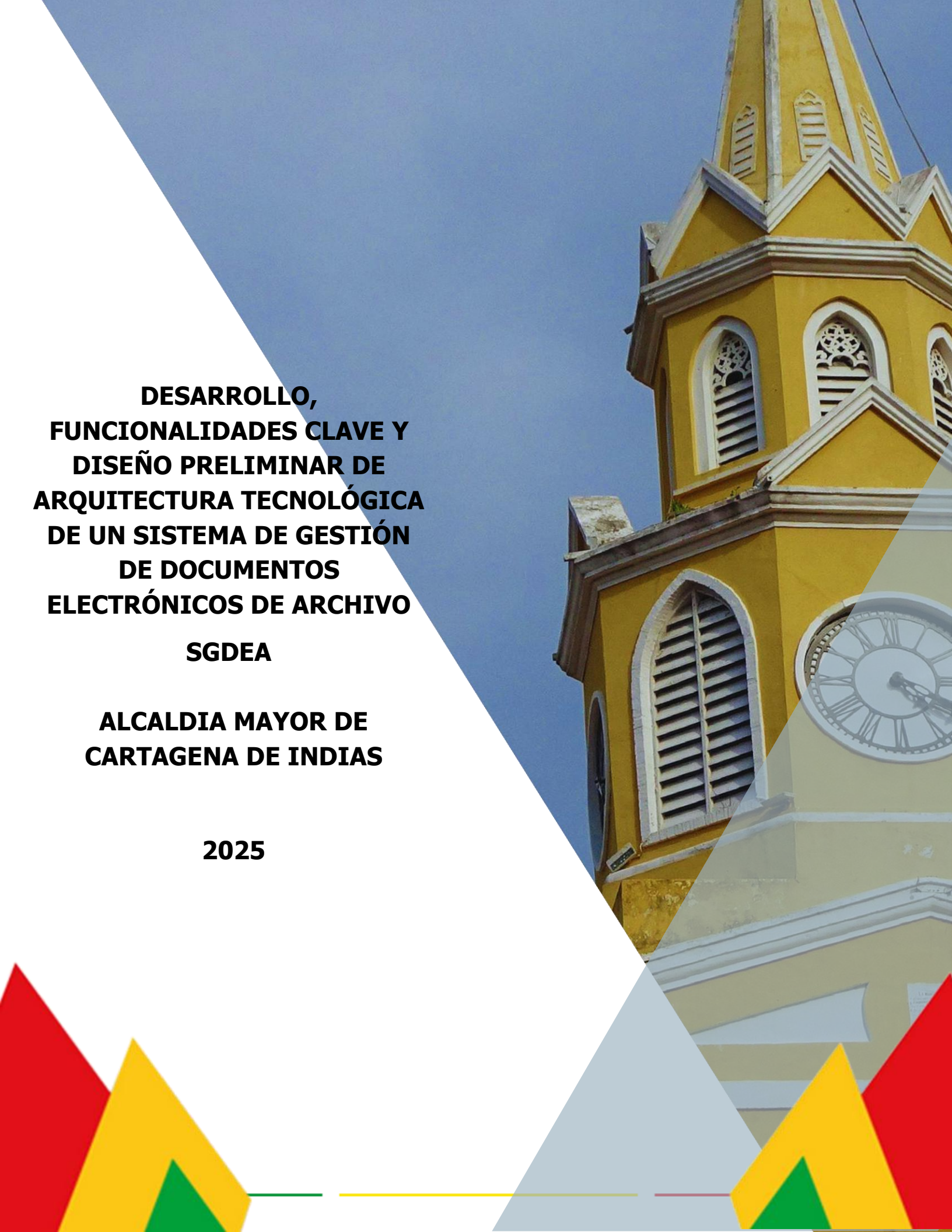


DESARROLLO, FUNCIONALIDADES CLAVE Y DISEÑO PRELIMINAR DE ARQUITECTURA TECNOLÓGICA DE UN SISTEMA DE GESTIÓN DE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

SGDEA

ALCALDIA MAYOR DE CARTAGENA DE INDIAS

2025

ARQUITECTURA

SISTEMAS DE GESTIÓN DE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO- SGDEA

DUMEK TURBAY PAZ
ALCALDE MAYOR DE CARTAGENA DE INDIAS

MARIA PATRICIA PORRAS MENDOZA
SECRETARIA GENERAL

JOSÉ CARLOS PUELLO RUBIO
DIRECTOR DE ARCHIVO GENERAL

CARTAGENA DE INDIAS

Tabla de Contenido

1. INTRODUCCIÓN

El Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA) se presenta como un marco integral para la gestión de documentos electrónicos producidos o recibidos por las entidades públicas, abarcando su ciclo de vida completo: planeación, producción e ingreso, gestión y trámite, organización, transferencia, disposición final y preservación a largo plazo. Este enfoque está alineado con la normativa colombiana vigente, en particular la Ley 594 de 2000 (Ley General de Archivos), el Decreto 2609 de 2012 y el Decreto 1080 de 2015, así como con las guías y estándares del Archivo General de la Nación (AGN).

Adicionalmente, el SGDEA incorpora buenas prácticas internacionales en gestión documental, tales como el modelo de referencia OAIS (ISO 14721) para archivos abiertos, y las normas ISO 15489 e ISO 30301 sobre gestión de documentos y sistemas de gestión de registros. De este modo, se busca garantizar que la autenticidad, la integridad, la confiabilidad, la disponibilidad y la trazabilidad de los documentos se mantengan a lo largo del tiempo, y que dichos documentos conserven su valor probatorio, administrativo, legal e histórico.

En el caso específico de la Alcaldía Mayor de Cartagena de Indias, el SGDEA se concibe como una herramienta estratégica para apoyar el proceso de diagnóstico, diseño e implementación de la gestión documental electrónica, en el marco de la transformación digital de la administración pública. Esta entidad produce y recibe diariamente un alto volumen de información asociada a trámites ciudadanos, contratación, planeación, hacienda, talento humano, servicios públicos, obras, programas sociales y demás procesos misionales y de apoyo, por lo cual la gestión sistemática de sus documentos electrónicos es crítica para asegurar una administración eficiente, transparente y orientada al ciudadano.

En este sentido, el SGDEA no es solo una solución tecnológica aislada, sino un sistema de gobernanza documental que integra:

- Políticas, procedimientos y normas internas.
- Recursos tecnológicos (software, hardware, redes, almacenamiento).
- Recursos humanos (roles, responsabilidades, competencias).
- Mecanismos de coordinación con otros sistemas institucionales.

El diseño del SGDEA busca responder a la creciente necesidad de transformación digital del sector público, promoviendo una gestión documental más eficiente, transparente y confiable. Al incorporar controles de seguridad, mecanismos de auditoría y políticas de preservación digital, se pretende no solo cumplir con los requerimientos legales, sino también fortalecer la memoria institucional de la alcaldía, garantizar la defensa jurídica de la misma entidad, mejorar la rendición de cuentas ante la ciudadanía y los entes de control, como también, consolidar un patrimonio documental digital robusto y accesible.

Este documento detalla el alcance, los objetivos y la estructura del SGDEA, así como el desarrollo técnico y funcional del sistema, las funcionalidades clave requeridas y un diseño preliminar de la arquitectura tecnológica para su implementación. Dado que la Alcaldía se encuentra en fase de diagnóstico inicial, se formulan lineamientos amplios que orientan tanto la posible adquisición de una solución como el eventual desarrollo interno o a la medida, enfatizando siempre la seguridad, la interoperabilidad y la sostenibilidad del sistema.

En retrospectiva, el SGDEA para la Alcaldía de Cartagena trasciende su rol inicial de cumplimiento normativo para convertirse en el eje central de la inteligencia institucional y cívica. En el futuro, sus atributos clave serán la autonomía predictiva impulsada por la Inteligencia Artificial, que no solo gestionará documentos, sino que anticipará necesidades legales y administrativas. La inmutabilidad de su patrimonio documental, respaldada por tecnologías de registro distribuido (*blockchain*), garantizará una transparencia total y una trazabilidad inquebrantable para la ciudadanía. Finalmente, el SGDEA se consolidará como una Plataforma de Conocimiento plenamente interoperable, transformando la memoria de La Heroica en un activo digital dinámico que facilita la toma de decisiones proactiva y sostiene una administración pública eficiente, confiable y orientada al futuro.

2. ALCANCE

El alcance del SGDEA abarca la creación de un sistema de gobernanza documental (no solo tecnológico) que garantice el manejo eficiente, transparente y normativo de los documentos electrónicos de la Alcaldía Mayor de Cartagena de Indias, apoyando su transformación digital y cumpliendo con objetivos

legales, administrativos e históricos. Este alcance incluye la cobertura de todo el ciclo de vida del documento, desde la planeación, producción y gestión, hasta la transferencia, disposición final y preservación a largo plazo, en todas las dependencias misionales y de apoyo de la entidad. Asimismo, involucra la integración de políticas internas, recursos tecnológicos (software, hardware, almacenamiento seguro) y la capacitación del talento humano, asegurando la autenticidad, integridad, confiabilidad, disponibilidad y trazabilidad de la información institucional.

2.1. Enfoque geográfico y normativo

- Contexto principal: Colombia, con atención específica en la Alcaldía Mayor de Cartagena de Indias, que inicia su proceso de diagnóstico y diseño de un SGDEA.
- Cobertura normativa:
    - Ley 594 de 2000 (Ley General de Archivos). marco normativo vigente al que se alinea el SGDEA.
    - Decreto 2609 de 2012 regula aspectos de la gestión documental y el ciclo de vida de los documentos, haciendo hincapié en la gestión de documentos electrónicos.
    - Decreto 1080 de 2015 (Decreto Único Reglamentario del Sector Cultura, que incluye disposiciones sobre SGDEA y documentos electrónicos): establece directrices para la protección, conservación y difusión del patrimonio documental de la nación y detalla el reglamento operativo y técnico.
    - Lineamientos, acuerdos y guías técnicas del Archivo General de la Nación (AGN): el SGDEA debe alinearse con las guías y estándares del AGN, incorporando criterios técnicos, metadatos, formatos de archivo y procesos de digitalización certificados.
    - Ley 1581 de 2012 y normas relacionadas con la protección de datos personales. las entidades públicas deben garantizar que los datos personales contenidos en documentos no sean divulgados sin autorización, y se deben proteger su integridad y disponibilidad.

- Normas técnicas de seguridad de la información (p. ej. ISO/IEC 27001): marco de referencia para confiabilidad, integridad y disponibilidad, asegurando que solo personas autorizadas accedan a los documentos y que estos no se alteren.

El alcance se limita al sector público colombiano, particularmente a la realidad institucional de una Alcaldía Mayor de Cartagena de Indias. No se incluyen marcos regulatorios estrictamente privados ni contextos normativos de otros países, aunque sí se citan buenas prácticas internacionales a modo de referencia, dado a su importancia.

2.2. Alcance contextual y lecciones aprendidas del sector público colombiano

Este apartado contextualiza el alcance del SGDEA tomando como base las experiencias y prácticas relevantes del sector público colombiano. Su propósito es orientar la definición de límites, criterios de adopción y prioridades de diseño e implementación.

- ORFEO y sistemas derivados (p. ej., SGDEA-RGO): experiencias en gestión de correspondencia y documentos oficiales que permiten mejorar la trazabilidad, reducir tiempos de respuesta y facilitar el acceso remoto. Se priorizará la adopción de patrones de flujo de trabajo, estructuras de metadatos y controles de seguridad que hayan demostrado efectividad.

- Lineamientos de interoperabilidad y gobierno digital (Función Pública, MinTIC, Colombia Compra Eficiente - SECOP, SIGEP y otros): estos lineamientos serven como marco para la interoperabilidad, la gobernanza de datos y la entrega de servicios digitales al ciudadano. Se adoptaron principios de interoperabilidad, estándares de metadatos y políticas de acceso conforme a las directrices oficiales.

- Casos de integración entre sistemas (trámite, contratación, talento humano y archivo electrónico): se considerarán modelos de integración probados para definir arquitecturas, APIs y mecanismos de transferencia

de información entre sistemas críticos, priorizando la consistencia de metadatos y la seguridad.

- Lecciones de gestión del cambio y capacitación: prácticas exitosas de adopción tecnológica, manejo de resistencia al cambio, desarrollo de capacidades y gobernanza de roles. Estas lecciones guiarán el plan de capacitación y la gestión de recursos humanos durante la implementación.

¿Cómo estas experiencias definen el alcance y las fronteras del SGDEA?

- Criterios de adopción: se incorporarán prácticas probadas en interoperabilidad, seguridad de la información y modelos de metadatos alineados con estándares del AGN, siempre que sean compatibles con la normativa local y las capacidades de la Alcaldía.
- Criterios de exclusión derivados de experiencias: se evitarán integraciones con plataformas privadas no reguladas por la AGN o no alineadas con las políticas de gobierno digital; se priorizará la integración con sistemas institucionales críticos (trámite, contratación, talento humano y correspondencia) y se descartarán soluciones que no aporten interoperabilidad o trazabilidad relevantes.
- Horizonte de implementación: las lecciones aprendidas orientan la hoja de ruta y fases de implementación (diagnóstico, diseño, prueba de concepto, despliegue gradual y escalamiento), así como las áreas prioritarias (flujos de trabajo, metadatos, preservación y seguridad).

Propósito práctico para el SGDEA

- Basar decisiones de arquitectura e integración en experiencias probadas, reduciendo incertidumbres y riesgos.
- Definir explícitamente lo que se adoptará, lo que se adaptará y lo que no se abordará, con criterios claros para cada caso.
- Garantizar coherencia con las guías de AGN y con las políticas de gobierno digital y protección de datos.

2.3. Exclusiones explícitas

El alcance del presente SGDEA está estrictamente delimitado al ámbito y operación de la Alcaldía Mayor de Cartagena de Indias y por extensión, al sector público colombiano según lo dictamina el Archivo General de la Nación (AGN). Por consiguiente, se excluye explícitamente cualquier implementación o adaptación del sistema para operar en jurisdicciones o entidades que no pertenezcan a la administración pública en Colombia. No se incluye un análisis o profundización en regulaciones exclusivas del sector privado, tales como aquellas de comercio electrónico o bancarias, que no posean una correspondencia directa con la normatividad archivística oficial del país (Ley 594 de 2000 y decretos complementarios). Asimismo, la arquitectura y los lineamientos del SGDEA no incorporan, ni desarrollan, normas técnicas o legales extranjeras que no hayan sido adoptadas, referenciadas o validadas de manera explícita por las autoridades competentes colombianas. Este enfoque garantiza que la solución sea jurídicamente sólida y aplicable únicamente al contexto legal y funcional para el cual fue diseñada.

2.4. Cobertura funcional del ciclo documental

El Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA) está diseñado para gestionar de manera integral, segura y normalizada todas las fases del ciclo vital de los documentos electrónicos, garantizando el cumplimiento normativo y la preservación de su valor probatorio y patrimonial. La cobertura funcional detallada se estructura de la siguiente manera:

- **Planeación y diseño archivístico**
    - Definición y Normalización de Esquemas Documentales: Establecimiento del cuadro de clasificación documental (CCD), con la definición detallada de series, subseries y tipos documentales, alineados con las Tablas de Retención Documental (TRD) vigentes.
    - Ingeniería de Formularios Electrónicos: Diseño e implementación de formularios digitales para la captura estructurada y validada de

información en el punto de origen, asegurando la integridad y consistencia de los datos.

- Especificación de Esquemas de Metadatos: Definición de perfiles de metadatos administrativos, descriptivos, técnicos y de preservación, acordes con los estándares del AGN (p. ej., Norma Técnica de Descripción Archivística) y modelos internacionales como Dublin Core o PREMIS.
- Modelado y Parametrización de Flujos de Trabajo (Workflow): Configuración de reglas de negocio, rutas de tramitación, condiciones, plazos y roles asociados a cada tipo documental o procedimiento administrativo.

- **Producción / Ingreso**

  - Ingreso Multicanal: Captura y registro centralizado de documentos provenientes de diversas fuentes: digitalización certificada de documentos físicos (cumpliendo normas del AGN), correos electrónicos, formularios web, APIs de sistemas transaccionales y documentos nativos digitales.
  - Generación y Control de Documentos Salientes: Creación de documentos oficiales (oficios, resoluciones, actos administrativos) con incorporación automática de sellos de tiempo, marcas de agua digitales y otros elementos de seguridad.
  - Radicación e Identificación Única: Asignación automática e irrevocable de códigos únicos de radicación (NUR - Número Único de Radicación) que garantizan la trazabilidad absoluta del documento a lo largo de todo su ciclo de vida.

- **Gestión, tramitación y distribución**

  - Distribución Inteligente y Asignación Automatizada: Enrutamiento digital de documentos y expedientes a unidades administrativas o funcionarios específicos, basado en reglas predefinidas (por competencia, materia, disponibilidad).
  - Gestión de Tareas y Seguimiento en Tiempo Real: Control detallado del estado del trámite, tiempos de respuesta, historial de movimientos,

responsables actuales y anteriores, mediante dashboards e indicadores de gestión.

- Motor de Notificaciones y Alertas Proactivas: Sistema de comunicaciones automatizadas (notificaciones push, correos electrónicos, alertas en sistema) para recordatorios de tareas pendientes, vencimiento de términos y cambios de estado críticos.

- **Organización, clasificación y descripción**

  - Clasificación Archivística Automatizada: Aplicación automática de códigos de clasificación del CCD a los documentos ingresados, facilitando su organización lógica.
  - Conformación y Gestión de Expedientes Electrónicos: Agrupación dinámica de todos los documentos relacionados con un mismo asunto, caso o procedimiento, manteniendo el contexto orgánico-funcional.
  - Control Estricto de Versiones: Registro del historial de modificaciones de un documento, con almacenamiento de versiones anteriores, identificación del autor del cambio y timestamp, garantizando la inmutabilidad de las versiones finales.
  - Descripción Archivística Enriquecida: Aplicación de instrumentos de descripción (inventarios, catálogos, guías) mediante la explotación de los metadatos capturados.

- **Transferencia y remisión documental**

  - Transferencia Primaria/Secundaria Controlada: Gestión del paso formal de documentos y expedientes desde el archivo de gestión al archivo central o intermedio, y de este al archivo histórico, generando los instrumentos de transferencia requeridos (actas, inventarios).
  - Interoperabilidad para Transferencia entre Sistemas: Mecanismos seguros (APIs, servicios web) para la transferencia automatizada de documentos y sus metadatos desde sistemas transaccionales (p. ej., sistemas de contratación, trámites) hacia el repositorio del SGDEA, asegurando la integridad de la información.

- **Disposición final y eliminación**

    - Ejecución de las Tablas de Retención Documental (TRD): Aplicación automatizada o semiautomatizada de las decisiones de disposición final (conservación permanente, eliminación, selección, micro digitación) una vez cumplidos los plazos de retención establecidos en la TRD.
    - Gestión de Procesos de Eliminación: Registro auditable de todo el proceso de baja documental, incluyendo la generación de actas de eliminación, listados de documentos eliminados y evidencias que demuestran el cumplimiento del procedimiento legal.

- **Preservación digital a largo plazo**

    - Gestión Proactiva de Formatos: Implementación de políticas de formatos de archivo (preferidos, aceptados, de preservación) y ejecución de planes de migración periódica para combatir la obsolescencia tecnológica.
    - Metadatos de Preservación (PREMIS): Generación, almacenamiento y gestión de metadatos técnicos específicos para preservación (checksums, información de formatos, agentes de software/hardware) que documenten la procedencia y autenticidad del objeto digital a lo largo del tiempo.
    - Verificación de Integridad y Autenticidad: Ejecución de rutinas periódicas de checksum (hashes criptográficos como SHA-256) para detectar corrupción o alteración no autorizada de los documentos preservados.
    - Almacenamiento de Preservación Seguro: Conservación de los documentos de valor permanente en repositorios especializados con infraestructura redundante, copias de seguridad georeplicadas y controles ambientales y de acceso reforzados, garantizando su perpetuidad y accesibilidad futura.

2.5. Interoperabilidad institucional

El SGDEA se concibe no como un sistema aislado, sino como el núcleo del ecosistema digital de la entidad, articulándose de manera estratégica y segura con los sistemas de información críticos para los procesos misionales y de apoyo. La interoperabilidad es un principio fundamental para evitar silos de información, eliminar la redundancia en la captura de datos y garantizar la unicidad, trazabilidad y autenticidad de los documentos en todo el entramado institucional.

Sistemas Objetivo de Integración Prioritaria:

- **SIGEP (Sistema de Gestión del Empleo Público):** Intercambio bidireccional para asociar documentos electrónicos (actos administrativos, hojas de vida, certificaciones) a los registros de servidores públicos, permitiendo la gestión integral del ciclo laboral y fortaleciendo los procesos de control interno y transparencia.
- **SECOP I/II (Sistema Electrónico de Contratación Pública):** Integración con el ciclo de la contratación estatal. El SGDEA actuará como repositorio oficial y de preservación de los documentos generados en los procesos de precontractual, contractual y poscontractual (pliegos, actas, contratos, informes de interventoría), garantizando su inmutabilidad y valor probatorio a largo plazo.
- **Sistemas de Gestión Documental y Correspondencia:** En escenarios de implementación progresiva o coexistencia, se establecerán mecanismos de interoperabilidad para la migración o transferencia controlada de documentos y metadatos, asegurando la continuidad en la gestión y la homogeneización de prácticas archivísticas.
- **Aplicativos Internos Sectoriales (Finanzas, Talento Humano, Planeación, PQRSD, etc.):** La integración se desarrollará en función de los hallazgos del diagnóstico, priorizando los flujos documentales críticos. El objetivo es que estos sistemas se conecten al SGDEA como *fuentes de ingreso* de documentos electrónicos y como *consumidores* de información archivística confiable.

Arquitectura Técnica y Protocolos de Interoperabilidad:

La interoperabilidad se materializará mediante una capa de servicios robusta y estandarizada, que priorizará:

- APIs RESTful y Servicios Web (SOAP) Estandarizados: Implementación de interfaces de programación de aplicaciones (APIs) modernas, well-defined y documentadas, utilizando estándares abiertos (OpenAPI/Swagger) para facilitar el desarrollo, consumo y gobierno de los servicios de integración.
- Esquemas de Autenticación y Autorización Seguros: Empleo de protocolos de seguridad industriales como OAuth 2.0 y OpenID Connect para la autenticación entre sistemas (M2M - Machine to Machine) y la gestión de permisos granular, asegurando que cada aplicación acceda solo a los recursos documentales estrictamente autorizados.
- Formatos de Datos Abiertos y Estructuras de Metadatos Comunes: Utilización de formatos de intercambio ligeros y estructurados (JSON, XML) y adherencia a esquemas de metadatos comunes previamente definidos (por ejemplo, perfiles de metadatos del AGN o esquemas propios basados en Dublin Core), garantizando la semántica consistente y el correcto entendimiento de la información intercambiada entre sistemas heterogéneos.
- Event-Driven Architecture y Colas de Mensajería: Para escenarios que requieran alta escalabilidad y procesamiento asíncrono, se implementarán mecanismos basados en eventos (event-driven) y brokers de mensajería (como RabbitMQ o Apache Kafka), que notificarán a los sistemas suscriptores sobre eventos críticos del ciclo de vida documental (ej: documento radicado, expediente cerrado, documento transferido).

2.6. Alcance de conservación, autenticidad y seguridad

El SGDEA debe establecer un marco técnico, procedimental y normativo robusto que garantice de manera irrefutable las propiedades intrínsecas de los documentos electrónicos de archivo, asegurando su validez jurídica, operativa e

histórica a lo largo de todo su ciclo de vida. Este alcance se materializa en los siguientes pilares fundamentales:

- Autenticidad Garantizada: Implementación de mecanismos criptográficos y de control que certifiquen la autoría, origen y procedencia del documento. Esto incluye el uso de sellos de tiempo electrónico calificado (TSA), firmas digitales avanzadas (según Decreto 1074 de 2015), y metadatos de contexto que capturen información de creación (usuario, sistema, fecha-hora, acción realizada), asegurando que el documento es genuino y puede ser admitido como prueba en procedimientos legales o administrativos.
- Integridad Inmutable: Protección absoluta contra alteraciones no autorizadas, mediante la aplicación de funciones hash criptográficas (SHA-256, SHA-3) al momento de la captura o versión final. Cualquier modificación posterior genera un nuevo hash, invalidando la versión anterior y dejando una traza auditable. Se implementarán políticas de WORM (Write Once, Read Many) en los repositorios de conservación para prevenir la sobreescritura o eliminación accidental o malintencionada.
- Confiabilidad y Fiabilidad Probadora: Diseño de procesos que aseguren que el documento es una representación completa y exacta de la transacción, actividad o hecho que registra. Esto se logra mediante la integración directa con sistemas transaccionales fuente (evitando re-digitaciones), la validación de datos en el punto de ingreso y la aplicación estricta de procedimientos operativos estandarizados (SOPs), alineados con las normas ISO 15489 e ISO 30301, para respaldar su valor probatorio.
- Trazabilidad Completa y Auditoría Continua: Registro detallado e inalterable de todo evento significativo en la vida del documento (log de auditoría forense), incluyendo creación, modificación, acceso, transferencia, eliminación, así como la identidad del actor, fecha-hora exacta y justificación. Esto permite la reconstrucción forense de la cadena de custodia para fines de control interno, investigaciones disciplinarias o requerimientos judiciales.

- Seguridad de la Información (CID) y Protección de Datos: Implementación de un modelo de seguridad integral basado en la tríada CID:
    - Confidencialidad: Cifrado de datos en reposo (AES-256) y en tránsito (TLS 1.3+), control de acceso basado en roles (RBAC) y atributos (ABAC), con segregación de datos sensibles según normativa Ley 1581 de 2012 y Decreto 1377 de 2013.
    - Integridad: Mecanismos ya descritos (hashes, WORM).
    - Disponibilidad: Arquitectura de alta disponibilidad, planes de recuperación ante desastres (DRP) y respaldos automatizados y georeplicados para garantizar el acceso continuo a la información crítica. Este modelo se alineará con estándares internacionales como ISO/IEC 27001 y los marcos del Esquema Nacional de Seguridad Digital.

2.7. Alcance de gobernanza, seguridad y calidad

El SGDEA requiere un marco de gobernanza sólido que defina las reglas de juego, los roles, las políticas y los estándares que aseguren su operación efectiva, escalable y alineada con los objetivos institucionales a mediano y largo plazo.

- Modelo de Gobernanza y Roles Claramente Definidos: Establecimiento formal de un Comité de Gestión Documental Electrónica con representación de:
    - Archivo General: Liderazgo en políticas archivísticas, TRD, clasificación y preservación.
    - Oficina de Tecnologías de la Información (TI): Responsable de la infraestructura, seguridad técnica, integración y operación del sistema.
    - Áreas Misionales y de Apoyo: Propietarias de los procesos y la información, responsables de la calidad del ingreso y uso correcto del sistema.
    - Oficina Jurídica: Aseguramiento del cumplimiento normativo y valor probatorio.
    - Secretaría de Planeación / Control Interno: Definición de indicadores y auditoría de procesos.

- Políticas y Procedimientos Estandarizados: Documentación formal de:

    - Políticas de Retención y Disposición Final: Basadas en las TRD, con procesos de revisión y actualización periódica.
    - Esquemas de Metadatos: Modelos integrales que incluyan metadatos descriptivos (para búsqueda), administrativos (para gestión), estructurales (para empaquetado) y de preservación (PREMIS, para conservación a largo plazo).
    - Políticas de Calidad de la Información: Reglas de validación, normalización, limpieza y verificación de datos para garantizar la consistencia, exactitud y completitud de la información capturada.

- Auditoría, Control y Rendición de Cuentas: Diseño de registros de auditoría exhaustivos y capacidades de reporting que generen dashboards e informes automáticos para:

    - Control Interno: Monitoreo de eficiencia en trámites, cumplimiento de términos, uso del sistema.
    - Entes de Control Externa (Contraloría, Procuraduría): Facilitar el acceso evidentemente a documentos y sus trazas de auditoría.
    - Transparencia y Datos Abiertos: Generación de conjuntos de datos anonimizados para publicación.

- Arquitectura Escalable y Sostenibilidad Técnico-Financiera: El diseño del SGDEA considerará un horizonte de planificación mínimo de 5 años, priorizando:

    - Escalabilidad: Capacidad de crecer en volumen de documentos, usuarios concurrentes y complejidad de procesos sin requerir rediseños costosos (arquitecturas modulares, microservicios, almacenamiento escalable).
    - Sostenibilidad: Evaluación de Total Cost of Ownership (TCO), que incluye costos de licenciamiento, infraestructura, mantenimiento, operación y capacitación continua. Se priorizarán estándares abiertos y tecnologías con una curva de aprendizaje y mantenimiento razonable para la entidad.
    - Interoperabilidad Futura: Capacidad nativa para adaptarse a nuevos estándares e integrarse con sistemas futuros, evitando la obsolescencia tecnológica.

2.8. Alcance técnico y de interoperabilidad

El alcance técnico del SGDEA implica una rigurosa evaluación de las opciones de infraestructura, sopesando las ventajas de la nube pública, la nube privada, la infraestructura local y los esquemas híbridos, para garantizar la máxima eficiencia operativa y financiera. Se procederá a la definición detallada de requerimientos de seguridad, rendimiento y capacidad, que servirán de base para la selección de la solución tecnológica. La estrategia de preservación a largo plazo se asegurará mediante la adopción estricta de formatos abiertos y estándares archivísticos reconocidos internacionalmente, tales como PDF/A, XML, METS, Dublin Core y PREMIS. Paralelamente, la interoperabilidad será garantizada mediante el diseño de Interfaces de Programación de Aplicaciones (APIs) robustas y seguras, implementando mecanismos de autenticación avanzada como OAuth2 o mTLS. Finalmente, todo el sistema será anclado en un marco de seguridad de la información basado en la norma ISO/IEC 27001, asegurando la confidencialidad, integridad y disponibilidad del patrimonio documental de la Alcaldía.

2.9. Alcance de preservación digital

El alcance de la preservación digital en el SGDEA se rige por la adopción estricta de prácticas y principios basados en el modelo OAIS (ISO 14721), asegurando la supervivencia de la información a largo plazo a través de la gestión de Paquetes de Información de Archivo (AIP). Esta estrategia está plenamente alineada con las normas ISO 15489 e ISO 30301, garantizando que los documentos conserven su autenticidad, integridad y valor probatorio a lo largo del tiempo. Un componente crítico es el desarrollo e implementación de planes rigurosos de migración de formatos y verificación continua de la integridad mediante hashing y checksums, para combatir la obsolescencia tecnológica. Además, se establecerán políticas robustas de almacenamiento redundante a través de la replicación de datos en diferentes medios y esencialmente, la replicación geográfica de los archivos digitales, maximizando la disponibilidad y la protección ante desastres para el patrimonio documental de la Alcaldía.

2.10. Enfoque de implementación y pruebas

El alcance de la implementación del SGDEA adoptará un enfoque gradual y metódico, priorizando la estabilidad y la validación antes de la adopción total. Esto incluye la realización de proyectos piloto rigurosos dentro de dependencias seleccionadas, cruciales para validar la funcionalidad completa del sistema y la efectividad de la nueva gobernanza documental en un entorno controlado, minimizando riesgos operativos. El despliegue a gran escala solo procederá tras una estricta alineación con los lineamientos internos de la entidad, incluyendo la gestión de cambio y la capacitación de usuarios. La implementación requerirá la aprobación formal de la alta dirección de la Alcaldía para asegurar el compromiso institucional. Finalmente, se procederá a la definición clara de criterios de aceptación y la medición de resultados mediante indicadores de desempeño (KPIs) específicos, garantizando que el sistema entregue los beneficios esperados en eficiencia, transparencia y confiabilidad.

3. OBJETIVO GENERAL

Desarrollar, implementar y poner en operación un Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA) integral para la Alcaldía Mayor de Cartagena de Indias que garantice de manera continua la autenticidad, integridad, disponibilidad, confidencialidad y trazabilidad de los documentos electrónicos institucionales durante todo su ciclo de vida (desde la planeación y creación hasta la disposición final o preservación permanente), donde se asegure el cumplimiento riguroso de la normativa archivística, de gobierno digital y de protección de datos personales vigente en Colombia, así como de las directrices del Archivo General de la Nación y demás autoridades competentes, permitiendo la interoperabilidad técnica, semántica y organizacional con otros sistemas de información públicos (nacionales y locales), mediante el uso de estándares abiertos de formatos, metadatos y servicios web seguros, evitando la duplicidad de registros y esfuerzos.

Con el fin que contribuya a la modernización, eficiencia y transparencia de la gestión pública municipal, optimizando tiempos, recursos y calidad de los procesos administrativos y misionales, y mejorando la atención al ciudadano.

Asegurando la preservación a largo plazo del patrimonio documental digital de la Alcaldía, consolidando una memoria institucional confiable, accesible y reutilizable para la toma de decisiones, la investigación, el control social y la protección de derechos.

Por último, es importante implementar un modelo de gobernanza documental sólido que defina claramente los roles, responsabilidades, y competencias del talento humano, junto con un plan de capacitación y gestión del cambio que asegure la correcta adopción por todas las dependencias. Además, la arquitectura deberá garantizar la sostenibilidad técnico-financiera y la escalabilidad del sistema, minimizando el Costo Total de Propiedad (TCO) y preparándolo para el crecimiento futuro en volumen y complejidad. Finalmente, para garantizar el control y la transparencia, el SGDEA debe establecer mecanismos de auditoría exhaustivos y capacidades de *reporting* que faciliten la medición de resultados mediante indicadores de desempeño (KPIs), asegurando la protección contra desastres mediante almacenamiento redundante y planes de recuperación (DRP), consolidando así la confiabilidad integral del sistema.

3.1. Objetivos específicos

Los objetivos específicos del proyecto de implementación del SGDEA están diseñados para traducir la visión estratégica en resultados tangibles, medibles y alineados con el marco normativo y técnico expuesto. Estos objetivos garantizarán el despliegue de un sistema robusto, integrado y sostenible, sirviendo como la hoja de ruta detallada para la Alcaldía Mayor de Cartagena de Indias. Cada objetivo específico aborda componentes críticos del alcance —desde la arquitectura técnica y la seguridad de la información, hasta la gobernanza y la gestión del cambio— asegurando que la solución final no solo cumpla con la normatividad colombiana y los estándares internacionales (OAIS, ISO 30301), sino que también optimice la eficiencia operativa y fortalezca la capacidad institucional para la preservación documental a largo plazo.

3.1.1. Automatización y modelado del ciclo documental

Modelar y automatizar los procesos del ciclo de vida documental electrónico es fundamental para la eficiencia del SGDEA. Este objetivo específico se centra en

Diseñar, documentar e implementar los flujos de trabajo (*workflows*) para cada fase del ciclo vital del documento (desde la planeación y creación hasta la preservación a largo plazo). Para lograr esto, se establecerán formalmente los siguientes componentes dentro del sistema de gobernanza documental.

- Procedimientos Operativos Estandarizados (SOPs): Se desarrollarán y documentarán los procedimientos operativos estandarizados para cada actividad del flujo de trabajo, asegurando la consistencia y la fiabilidad de la gestión documental en toda la Alcaldía.

- Roles y Responsabilidades Definidos: Se realizará la asignación clara y formal de roles y responsabilidades para el manejo documental, incluyendo perfiles como creador, responsable, tramitador, archivero y administrador, lo cual es esencial para el control y la trazabilidad.

- Puntos de Control Críticos: Se definirán e integrarán puntos de control críticos dentro de los *workflows* para garantizar la calidad del dato, la seguridad de la información y el cumplimiento normativo riguroso en cada etapa del ciclo documental.

3.1.2. Establecer mecanismos de control, auditoría y seguridad documental

Este objetivo específico se centra en la implementación de salvaguardas técnicas y procedimentales necesarias para mantener la autenticidad, integridad y confiabilidad del patrimonio documental de la Alcaldía. Su propósito es definir e integrar puntos de control críticos dentro de los workflows que garanticen la calidad del dato, la seguridad de la información y el cumplimiento normativo riguroso en cada etapa del ciclo documental. Para implementarlo se trabajará en:

- Implementación de mecanismos de integridad: Aplicación de funciones hash criptográficas (como SHA-256) al momento de la captura o versión final de cada documento, y la integración de políticas de WORM (Write Once, Read Many) para prevenir la sobreescritura o eliminación malintencionada en los repositorios de conservación.

- Garantía de Autenticidad: Uso de sellos de tiempo electrónico calificado y firmas digitales avanzadas (según el Decreto 1074 de 2015), complementados con metadatos de contexto que capturen de forma inalterable la información de creación (usuario, sistema, fecha-hora, acción realizada).
- Trazabilidad y Auditoría Continua: Diseño de un registro de auditoría forense detallado e inalterable de cada evento significativo en la vida del documento (acceso, modificación, transferencia, eliminación), lo que permite la reconstrucción completa de la cadena de custodia para fines judiciales o de control interno.
- Marco de Seguridad Integral: Implementación de un modelo de seguridad basado en la tríada CID (Confidencialidad, Integridad y Disponibilidad), alineado con ISO/IEC 27001, que incluye el cifrado de datos, el control de acceso basado en roles (RBAC) y el desarrollo de planes de recuperación ante desastres (DRP).

3.1.3. Garantizar el cumplimiento normativo y archivístico

El objetivo de este punto es asegurar la estricta alineación del SGDEA con el marco jurídico colombiano y las políticas internas de la Alcaldía de Cartagena, garantizando que el sistema opere dentro de la legalidad vigente. Esto se materializa mediante:

- Parametrización Automatizada de TRD: Se realizará la parametrización automatizada de las Tablas de Retención Documental (TRD) vigentes, lo cual permitirá la ejecución controlada y auditada de las disposiciones finales, tales como la eliminación, conservación o selección de documentos, una vez cumplidos los plazos de retención legalmente establecidos

- Adaptación a Lineamientos Técnicos del AGN: El sistema será adaptado rigurosamente a los lineamientos técnicos, acuerdos y guías del Archivo General de la Nación (AGN). Esto incluye la correcta adopción de formatos de preservación (como PDF/A), los esquemas de metadatos requeridos y los procesos de digitalización certificada, asegurando el valor probatorio del patrimonio documental.

- Implementación de Controles de Protección de Datos: Se implementarán controles específicos y robustos para la protección de datos personales en cumplimiento estricto de la Ley 1581 de 2012 y sus decretos reglamentarios, garantizando la confidencialidad y la segregación de datos sensibles para solo ser accesibles por personal autorizado.

3.1.4. Diseñar y desplegar una estrategia de interoperabilidad Institucional

Este objetivo se centra en desarrollar e implementar una capa de servicios de integración que permita al SGDEA operar no como un sistema aislado, sino como el núcleo articulador del ecosistema digital de la Alcaldía Mayor de Cartagena de Indias. Para lograr la interoperabilidad técnica, semántica y organizacional, se priorizará el desarrollo de APIs RESTful robustas, bien definidas y documentadas (utilizando estándares como OpenAPI/Swagger), esenciales para el intercambio bidireccional de documentos y metadatos con otros sistemas. Se establecerán protocolos de autenticación segura (OAuth 2.0 y OpenID Connect) para la comunicación sistema-a-sistema (M2M), garantizando la seguridad en el intercambio de información. La estrategia contempla la priorización de la integración con sistemas críticos del sector público colombiano, tales como SIGEP (para la gestión laboral), SECOP I/II (para el ciclo de la contratación), y los sistemas de gestión de correspondencia y PQRSD. Esto asegurará la trazabilidad absoluta del documento y evitará la duplicidad de registros y esfuerzos en toda la entidad.

3.1.5. Construir una arquitectura tecnológica escalable y resiliente

El objetivo es definir y desplegar una infraestructura técnica para el SGDEA que asegure el rendimiento óptimo, la alta disponibilidad y la evolución futura del sistema, mitigando los riesgos tecnológicos a largo plazo. Este punto se logra a través de las siguientes acciones clave:

- Diseño Modular y Escalable: Se adoptará un diseño modular y basado en microservicios para facilitar el mantenimiento continuo del sistema y la escalabilidad independiente de cada componente funcional. Esta

aproximación tecnológica permite al SGDEA adaptarse al crecimiento en volumen documental y número de usuarios sin requerir rediseños costosos.

- Selección del Modelo de Despliegue Óptimo: Se llevará a cabo una evaluación y selección rigurosa del modelo de despliegue más adecuado (infraestructura local, nube pública/privada o un esquema híbrido). La decisión se basará en un análisis exhaustivo de los costos totales de propiedad (TCO), los requerimientos de seguridad de la información y las capacidades técnicas institucionales existentes de la Alcaldía.

- Estrategia de Resiliencia y DRP: Se implementará una estrategia de alta disponibilidad (HA) y un plan de recuperación ante desastres (DRP) robusto. Esto garantiza la continuidad del negocio ante fallas críticas y asegura la preservación inalterable del patrimonio documental digital, mediante la aplicación de almacenamiento redundante y réplicas geográficas cuando sea posible.

3.1.6. Ejecutar un plan integral de gestión del cambio y capacitación

El objetivo es asegurar la adopción efectiva y el uso correcto del SGDEA por parte de la totalidad de los funcionarios de la Alcaldía Mayor de Cartagena de Indias, garantizando que el sistema de gobernanza documental sea eficiente y sostenible. Esto se logrará mediante un enfoque integral:

- Plan de comunicación y sensibilización: Se implementará un plan de comunicación y sensibilización continúa diseñado para evidenciar de manera clara y proactiva los beneficios del SGDEA en términos de eficiencia, transparencia y valor probatorio, gestionando la resistencia al cambio e impulsando la apropiación institucional.

- Programas de capacitación diferenciada: Se diseñarán y ejecutarán programas de capacitación diferenciada y especializada que se ajusten a los roles específicos (usuarios finales, administradores, archiveros,

auditores), asegurando que cada funcionario desarrolle las competencias necesarias para el manejo documental y el cumplimiento normativo.

- Material de apoyo y soporte ágil: Se asegurará la disponibilidad de recursos de consulta permanente, como la creación de material de apoyo (manuales, videos tutoriales y Preguntas Frecuentes - FAQs), junto con el establecimiento de canales de soporte ágiles para resolver dudas y garantizar la operación continua y el correcto uso del sistema.

3.1.7. Establecer un modelo de mejora continua basado en datos

El objetivo es implementar mecanismos para medir el desempeño, identificar oportunidades de optimización y asegurar la evolución continua del SGDEA, transformándolo en un sistema de aprendizaje activo dentro de la Alcaldía de Cartagena. Esto se logrará a través de la formalización de la gestión del rendimiento:

- Definición de indicadores clave de desempeño (KPIs): Se realizará la definición rigurosa de indicadores clave de desempeño (KPIs) cuantitativos y cualitativos, tales como el tiempo promedio de trámite documental, el volumen documental procesado por unidad, la tasa de incidencias de seguridad y la disponibilidad del sistema. Estos KPIs permitirán cuantificar el impacto real del SGDEA en la eficiencia administrativa.

- Generación de reportes automatizados: Se establecerá la capacidad de generación de *dashboards* y reportes automáticos que consoliden la información de rendimiento y cumplimiento. Estos reportes serán el insumo principal para la toma de decisiones por parte de la gerencia, los responsables de procesos y el comité de gobernanza documental.

- Revisiones periódicas de los procesos y políticas: Se implementará un ciclo formal de revisión periódica de los procesos, la tecnología y las políticas de gobernanza, permitiendo al SGDEA adaptarse de manera ágil a los cambios normativos (emitidos por el AGN o el marco legal), las evoluciones tecnológicas y las cambiantes necesidades operativas de la entidad.

3.1.8. Ejecutar la validación y pilotos de despliegue controlado

Ejecutar la validación funcional y operativa del SGDEA a través de proyectos piloto controlados para minimizar riesgos y asegurar la viabilidad del sistema antes del despliegue masivo. Esto implica:

- **Realización de pilotos rigurosos:** implementar y operar el SGDEA en dependencias seleccionadas (ej. Contratación y Archivo Central) para validar la funcionalidad completa, los flujos de trabajo automatizados y los mecanismos de gobernanza en un entorno real.

- **Validación de criterios de aceptación:** Evaluar formalmente el sistema piloto frente a los criterios de aceptación previamente definidos (funcionalidad, rendimiento, seguridad y cumplimiento normativo), asegurando la aprobación y el compromiso de la alta dirección y los usuarios clave.

- **Ajuste y optimización:** Utilizar los resultados de los pilotos para identificar lecciones aprendidas, realizar ajustes a los procedimientos operativos (SOPs), refinar los programas de capacitación y optimizar la arquitectura técnica antes de iniciar el despliegue a gran escala.

4. JUSTIFICACIÓN

La implementación del Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA) para la Alcaldía Mayor de Cartagena de Indias no es una opción, sino un imperativo legal, administrativo y cívico. El proyecto se justifica en la urgente necesidad de superar las ineficiencias operativas y los riesgos jurídicos asociados a la gestión documental tradicional, garantizando el estricto cumplimiento de la normativa colombiana (Ley 594 de 2000 y Ley de Transparencia 1712 de 2014). Además, constituye la pieza central para la transformación digital de la entidad, permitiendo la preservación a largo plazo del patrimonio documental de La Heroica, el fortalecimiento de la defensa jurídica

y crucialmente, la mejora sustancial de la rendición de cuentas y la calidad del servicio ofrecido a la ciudadanía.

4.1. Justificación normativa y de cumplimiento

La implementación de un SGDEA en la Alcaldía Mayor de Cartagena de Indias responde, en primer lugar, a una obligación legal de carácter inaplazable. El marco archivístico colombiano, encabezado por la Ley 594 de 2000, el Decreto 2609 de 2012 y el Decreto 1080 de 2015, establece la obligatoriedad para las entidades públicas de gestionar sus documentos electrónicos bajo principios técnicos rigurosos, asegurando su integridad, autenticidad y conservación a perpetuidad, e implementando Tablas de Retención Documental para la disposición final. Este mandato legal se refuerza con la Ley 1712 de 2014 (Ley de Transparencia), que exige mecanismos tecnológicos para garantizar el derecho fundamental de acceso a la información pública, y con la Ley 1581 de 2012 sobre protección de datos personales. El SGDEA no es solo una herramienta, sino el instrumento operacional indispensable que permite a la Alcaldía dar cumplimiento efectivo a este complejo conjunto de disposiciones, integrando controles de seguridad, metodologías y tecnologías validadas por el Archivo General de la Nación (AGN), facilitando así la supervisión y la verificación por parte de los entes de control y minimizando el riesgo de sanciones jurídicas.

4.2. Justificación institucional y estratégica

La Alcaldía Municipal, como instancia de gobierno local, administra recursos públicos, ejecuta políticas, programas y proyectos, y presta servicios esenciales a la comunidad. Estas funciones generan y requieren una gran cantidad de documentos (oficios, actos administrativos, contratos, informes, estudios, expedientes de proyectos, etc.) que:

- evidencian la actuación de la administración;
- soportan decisiones y responsabilidades;
- y son base para auditorías, procesos judiciales y control social.

Sin un sistema integral como el SGDEA, la información se dispersa, se duplica, se pierde o se vuelve inaccesible, afectando la eficacia y la legitimidad de la

gestión institucional. El SGDEA se justifica como una herramienta estratégica para:

- consolidar una política institucional de gestión documental;
- fortalecer la coordinación entre dependencias;
- respaldar la toma de decisiones basada en información confiable y oportuna.

4.3. Justificación operativa: eficiencia y optimización de procesos

En términos operativos, la gestión documental tradicional en la Alcaldía genera ineficiencias críticas, caracterizadas por retrasos significativos en la circulación de expedientes, la sobrecarga de tareas manuales como búsquedas, copias y distribución física, y la dificultad crónica para ubicar versiones actualizadas de documentos clave. Estos problemas no solo afectan la productividad de los funcionarios, sino que también generan un alto Costo Total de Propiedad (TCO) asociado al consumo de papel, transporte interno y almacenamiento físico.

El SGDEA, correctamente implementado, actúa como un catalizador de la eficiencia, permitiendo la automatización completa de los flujos de trabajo (*workflows*), notificaciones y recordatorios. Esto resulta en una reducción drástica en los tiempos de respuesta al ciudadano y en la simplificación de la búsqueda de documentos mediante la aplicación rigurosa de metadatos. La optimización redundará en una mayor productividad laboral, una disminución cuantificable en el uso de recursos y lo más importante, una mejora sustancial en la calidad y agilidad de los servicios municipales, lo cual se medirá y validará mediante la implementación de los Indicadores Clave de Desempeño (KPIs).

Todo ello redunda en mayor productividad de los funcionarios, mejor servicio al ciudadano y un uso más eficiente de los recursos públicos.

4.4. Justificación en términos de gestión del riesgo

La ausencia de un SGDEA o su implementación deficiente expone a la Alcaldía Mayor de Cartagena de Indias a un nivel inaceptable de riesgo probatorio, legal y operacional. Estos riesgos incluyen la pérdida irrecuperable de documentos

críticos debido a fallos tecnológicos, errores humanos o eventos de desastre natural; la alteración malintencionada o accidental de documentos con valor probatorio; y la imposibilidad de demostrar la cadena de custodia de la información en procesos judiciales, disciplinarios o de control. Adicionalmente, el riesgo se extiende a los incumplimientos de plazos legales y a las fugas de información confidencial o sensible, lo que impacta directamente en la privacidad de los ciudadanos (Ley 1581) y en la reputación institucional.

El SGDEA se justifica como la principal herramienta de blindaje institucional contra estos riesgos. Sus mecanismos intrínsecos de: respaldo y recuperación ante desastres (DRP), registro de auditoría forense y trazabilidad inmutable, controles de acceso estrictos basados en roles y perfiles, y cifrado y protección de datos, permiten mitigar significativamente la exposición. De esta forma, el sistema aporta un entorno controlado, supervisarle y legalmente defendible para la gestión de la información pública, asegurando la continuidad del negocio y la confianza ciudadana.

4.5. Justificación tecnológica

La Alcaldía se enfrenta al reto de integrarse a la transformación digital del Estado colombiano, que incluye:

- tramitación en línea de servicios;
- firma electrónica y digital;
- interoperabilidad entre plataformas públicas;
- gobierno y datos abiertos.

Sin un SGDEA:

- los esfuerzos de digitalización quedan fragmentados;
- los documentos electrónicos se dispersan entre múltiples sistemas sin coordinación;
- se dificulta asegurar la preservación a largo plazo.

La adopción de un SGDEA justifica:

- construir una base tecnológica común para la gestión de documentos;

- facilitar la interoperabilidad interna y externa;
- garantizar que los documentos electrónicos se gestionen con criterios archivísticos y no solo informáticos.

4.6. Justificación en términos de valor público y transparencia

Una gestión documental sólida tiene impacto directo en:

- la transparencia de la administración (acceso a información veraz y oportuna);
- el control social (posibilidad de seguimiento y vigilancia ciudadana);
- la protección de derechos (soporte documental de decisiones que afectan a personas y comunidades).

El SGDEA:

- facilita el acceso a documentos públicos;
- mejora la respuesta a solicitudes de información;
- contribuye a construir una memoria institucional accesible y confiable.

De esta manera, su implementación está justificada no solo por razones internas, sino también por su aporte a la construcción de confianza entre la ciudadanía y la administración municipal.

4.7 Justificación cívica, de transparencia y rendición de cuentas

Más allá del cumplimiento interno, la justificación del SGDEA radica en su profundo impacto cívico y social. La implementación de un sistema robusto es el mecanismo esencial para materializar el espíritu de la Ley de Transparencia y Acceso a la Información Pública (Ley 1712 de 2014). Al garantizar la trazabilidad inmutable y la disponibilidad oportuna de los documentos, el SGDEA simplifica el acceso del ciudadano a la información pública, transformando la rendición de cuentas en un proceso proactivo, verificable y continuo. Este sistema fomenta un Gobierno Abierto al facilitar la generación de datos abiertos y reporting transparente, fortaleciendo la confianza en la Alcaldía, promoviendo el control social efectivo y asegurando que las decisiones administrativas y el manejo de

los recursos públicos sean completamente transparentes para la comunidad de Cartagena.

5. DESARROLLO DEL SISTEMA DE GESTIÓN DE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO (SGDEA)

El desarrollo e implementación del SGDEA se concibe como un proyecto estratégico e integral, fundamental para la transformación digital de la Alcaldía. No se trata únicamente de la adquisición de una herramienta tecnológica, sino de la consolidación de un sistema de gobernanza documental que integra políticas, procesos, tecnología y personas. Este desarrollo debe estar alineado con el marco normativo colombiano (Ley 594 de 2000, Decreto 1080 de 2015), los lineamientos del Archivo General de la Nación (AGN) y las buenas prácticas internacionales (ISO 15489, ISO 30301).

El proyecto abarca las siguientes fases clave:

- Diagnóstico y análisis estratégico: Esta es la fase inicial y estratégica del proyecto SGDEA, diseñada para establecer la línea base y la hoja de ruta. Consiste en una evaluación exhaustiva y sistémica del estado actual de la gestión documental de la Alcaldía (procesos *as-is*, infraestructura tecnológica, capacidad de recursos humanos y cumplimiento normativo). Su propósito principal es identificar y documentar las brechas funcionales y de cumplimiento legal frente a la normativa colombiana (AGN) y los estándares internacionales (ISO). Además, esta fase incluye un análisis riguroso de viabilidad, que determina los requerimientos técnicos y funcionales detallados, y un estudio de Costo Total de Propiedad (TCO), cuyos resultados serán los únicos insumos válidos para la toma de decisiones sobre la adquisición, desarrollo a medida o selección de la solución tecnológica.
- Diseño funcional y técnico: Esta fase representa la ingeniería detallada del SGDEA, donde los requerimientos funcionales y técnicos identificados en el diagnóstico se traducen en especificaciones concretas para su construcción o adquisición. El Diseño Funcional define los flujos de trabajo (*workflows*) automatizados para cada etapa del ciclo de vida documental, la estructura de metadatos obligatorios (administrativos y de preservación) y el modelo de gobernanza documental con la asignación formal de roles

y permisos de acceso. Por su parte, el Diseño Técnico se enfoca en la arquitectura tecnológica modular y escalable (microservicios), la estrategia de interoperabilidad (especificación de APIs y protocolos de autenticación segura como OAuth2) y la definición de las políticas de seguridad (cifrado, control de acceso y alta disponibilidad), asegurando la alineación total con el marco ISO/IEC 27001 y los lineamientos del AGN.

- Selección o construcción de la solución tecnológica: Esta fase es crítica y se ejecuta una vez finalizado el diseño detallado, representando el punto de inflexión del proyecto. Implica la evaluación rigurosa de las alternativas para adquirir o construir la plataforma tecnológica del SGDEA. La decisión entre una solución existente (comercial o de *software* libre) o un desarrollo a la medida se basará en el análisis costo-beneficio realizado en la fase de diagnóstico, priorizando siempre la alineación funcional con los requerimientos específicos de la Alcaldía de Cartagena y el cumplimiento normativo colombiano. El principal objetivo es seleccionar la opción que garantice la sostenibilidad técnica y financiera a largo plazo, la máxima escalabilidad y la adhesión estricta a los estándares abiertos y de seguridad definidos en el diseño.
- Implementación progresiva y controlada: Esta fase abarca la puesta en marcha controlada del SGDEA, enfocándose en la minimización de riesgos operativos antes del despliegue masivo. Inicia con la ejecución de proyectos piloto rigurosos en dependencias seleccionadas, donde se realiza la configuración, integración de la arquitectura y la migración inicial de documentos. El objetivo primordial es validar la funcionalidad completa del sistema, la efectividad de los *workflows* automatizados y la nueva gobernanza documental, contrastándolos con los criterios de aceptación predefinidos (KPIs, rendimiento y seguridad). Solo tras obtener los resultados satisfactorios de estos pilotos y la aprobación formal de la alta dirección, se procede a la implementación progresiva al resto de la Alcaldía, asegurando que las lecciones aprendidas se incorporen para optimizar los procedimientos y garantizar una transición exitosa.
- Gestión del cambio organizacional y capacitación: Esta fase es fundamental y transversal, ya que aborda el factor humano, el cual es determinante para la sostenibilidad y el éxito a largo plazo del SGDEA. Consiste en la ejecución de un Plan Integral de Gestión del Cambio

Organizacional y de capacitación, diseñado para garantizar la adopción efectiva y el uso correcto del nuevo sistema y de la gobernanza documental por parte de la totalidad de los funcionarios de la Alcaldía. El plan incluye un componente de comunicación y sensibilización continua que gestiona proactivamente la resistencia y destaca los beneficios en eficiencia y transparencia. Se implementarán programas de capacitación diferenciada y especializada según los roles definidos (usuarios finales, archiveros, administradores), asegurando que cada perfil desarrolle las competencias necesarias. La culminación de esta fase implica la creación de material de apoyo permanente (manuales, videos) y canales de soporte ágiles, indispensables para asegurar la sostenibilidad operativa y la apropiación total del SGDEA.

La decisión de adquirir una plataforma existente (comercial o de software libre) o desarrollar una solución a medida se basará en los resultados del diagnóstico, un análisis riguroso de costo-beneficio y la alineación con las capacidades institucionales.

5.1 Fase de diagnóstico y análisis

Esta fase es la piedra angular y el cimiento estratégico del proyecto SGDEA, cuyo objetivo es crear una radiografía completa y sistémica de la gestión documental actual de la Alcaldía (procesos *as-is*, infraestructura tecnológica, capacidades de personal y marco normativo aplicado). Su importancia radica en que sienta las bases técnicas y financieras para toda decisión futura, permitiendo identificar y documentar con rigor las brechas funcionales y de cumplimiento legal frente a la normativa colombiana (AGN) y los estándares archivísticos internacionales. El entregable clave de esta fase es el análisis de viabilidad técnico-financiera, que incluye el estudio detallado del Costo Total de Propiedad (TCO), así como los requerimientos detallados del sistema. Los resultados de esta radiografía se convierten en los únicos insumos estratégicos válidos para fundamentar la decisión crucial sobre la adquisición de una plataforma existente o el desarrollo de una solución a la medida.

Para esto se debe levantar información sobre:

5.1.1. Procesos

El levantamiento de información sobre procesos constituye la auditoría funcional y operativa de la Alcaldía. Su propósito es realizar un mapeo exhaustivo de los procesos misionales (ej. licencias, trámites ciudadanos), estratégicos y de apoyo (ej. contratación, gestión humana, financiero). Este mapeo debe ir más allá de la mera descripción de actividades:

- Identificación de flujos y riesgos: Se debe documentar el flujo documental de cada proceso (*as-is*), identificando los puntos de control críticos, los cuellos de botella operativos (retrasos, tareas manuales) y las áreas de alto riesgo probatorio o legal donde la cadena de custodia es débil o inexistente.

- Definición de *Workflows*: Este análisis es el insumo principal para el posterior diseño de los *workflows* automatizados del SGDEA, estableciendo los procedimientos operativos estandarizados (SOPs) y la asignación formal de roles y responsabilidades (creador, tramitador, archivero).

- Vinculación con documentos y metadatos: Por cada actividad mapeada, se debe precisar qué documentos o evidencias electrónicas se producen o reciben, y qué metadatos esenciales (administrativos, descriptivos) son críticos para su trazabilidad y valor probatorio a lo largo de todo el ciclo de vida documental.

5.1.2. Universo documental:

El levantamiento del Universo Documental es crucial para la alineación archivística y el cumplimiento normativo del SGDEA. Este ejercicio implica la identificación, clasificación y cuantificación de todas las series, subseries y tipos

documentales que produce y recibe la Alcaldía de Cartagena, tanto en formato físico como electrónico.

- Alineación normativa: El objetivo principal es establecer la correspondencia estricta de este universo documental con las Tablas de Retención Documental (TRD) y de ser necesario, las Tablas de Valoración Documental (TVD) aprobadas por el Archivo General de la Nación (AGN).

- Diseño de metadatos: La información recopilada será el insumo fundamental para el diseño semántico del sistema, permitiendo definir los esquemas de metadatos obligatorios (administrativos, técnicos, descriptivos) que deben ser capturados automáticamente por el SGDEA para garantizar la autenticidad y la trazabilidad de cada registro.

- Estrategia de preservación y migración: Al identificar el volumen y el formato actual de los documentos (especialmente los históricos), se sientan las bases para el diseño de la estrategia de migración de formatos (ej. a PDF/A) y la estrategia de preservación a largo plazo conforme al modelo OAIS, asegurando que el patrimonio documental de la Alcaldía mantenga su valor probatorio a perpetuidad.

5.1.3. Volumetría:

El levantamiento de la Volumetría es un ejercicio técnico y financiero indispensable dentro de la fase de diagnóstico. Consiste en la cuantificación precisa de los volúmenes actuales de producción documental (tasas de ingreso diarias, semanales o mensuales) y del almacenamiento histórico total que posee la Alcaldía, tanto en formato físico como digital.

- Impacto en la inversión (TCO): El objetivo principal es fundamentar las decisiones de inversión en infraestructura. La Volumetría determina directamente los requerimientos de capacidad inmediata (almacenamiento, servidores, *backups*) y se convierte en el factor crítico para el cálculo preciso del Costo Total de Propiedad (TCO) del SGDEA.

- Diseño de la arquitectura: Esta información, complementada con proyecciones de crecimiento a mediano y largo plazo, es esencial para el diseño de una Arquitectura Tecnológica Escalable y Resiliente (Objetivo 4.5). Un análisis de volumetría deficiente puede afectar el rendimiento del sistema y comprometer la capacidad de los planes de recuperación ante desastres (DRP) y la alta disponibilidad.

- Modelo de despliegue: La volumetría es crucial para la evaluación y selección del modelo de despliegue óptimo (infraestructura local, nube pública o híbrida), garantizando que el sistema pueda soportar el crecimiento futuro de la Alcaldía sin incurrir en obsolescencia prematura.

5.1.4. Ecosistema tecnológico:

El levantamiento del Ecosistema Tecnológico es esencial para determinar la viabilidad técnica y la estrategia de interoperabilidad del SGDEA. Esta tarea implica la realización de un inventario exhaustivo de los sistemas de información existentes en la Alcaldía (ERP, sistemas de contratación como SECOP I/II, sistema de talento humano como SIGEP, sistemas de PQRSD), evaluando sus capacidades y limitaciones actuales. Paralelamente, se debe auditar la infraestructura de TI disponible (servidores, redes, *switches*, almacenamiento y políticas de *backup*). Esta información es crítica para:

- Diseño de integración: Especificar la capa de servicios necesaria, incluyendo el desarrollo de APIs RESTful y la definición de protocolos de autenticación segura (OAuth2), conforme al Objetivo 4.4 de Interoperabilidad.

- Selección arquitectónica: Determinar la capacidad real de la infraestructura local (*on-premise*) para soportar el SGDEA y tomar decisiones informadas sobre la necesidad de migrar a modelos de nube pública, privada o híbrida, vinculando este análisis directamente al cálculo del TCO y la arquitectura escalable (Objetivo 4.5).

- Análisis de riesgo: Evaluar las políticas de seguridad vigentes para identificar brechas y asegurar que el nuevo SGDEA se implemente bajo un marco robusto, alineado con ISO/IEC 27001, mitigando el riesgo de incidentes de seguridad y fallas de continuidad del negocio (DRP).

5.1.5. Capital humano:

El levantamiento de información sobre el Capital Humano es una fase crítica para la gestión del cambio y la sostenibilidad del SGDEA, ya que el factor humano es el eje de la correcta adopción del sistema. Consiste en la evaluación detallada de las capacidades y competencias del personal clave de la Alcaldía: el personal de archivo, el equipo de Tecnologías de la Información (TI) y los usuarios finales de las dependencias misionales.

- Diagnóstico de brechas: El objetivo es identificar las brechas de conocimiento en materia de gestión documental electrónica, normativa archivística colombiana y el manejo de nuevas herramientas digitales.

- Definición de roles de gobernanza: Los resultados de esta evaluación son el insumo principal para el diseño formal de la gobernanza documental y la asignación clara de roles y responsabilidades dentro del SGDEA.

- Plan de capacitación: Esta fase permite definir la estrategia de gestión del cambio, determinando la necesidad de programas de capacitación diferenciada y especializada que aseguren que cada perfil desarrolle las competencias requeridas para el uso correcto, eficiente y normativo del nuevo sistema.

5.1.6. Marco normativo interno y políticas vigentes

El objetivo es realizar una revisión y consolidación de todo el entramado regulatorio interno de la Alcaldía que afecta la producción, gestión y seguridad de los documentos.

- Identificación de políticas internas: se debe auditar y documentar formalmente el estado de los Manuales de Procesos y Procedimientos, los Reglamentos Internos de Archivo (si existen), las Políticas de Seguridad de la Información y los documentos relacionados con la privacidad y protección de datos ya vigentes en la Alcaldía.
- Análisis de integración: Esta revisión es fundamental para asegurar que el diseño del SGDEA (sus *workflows*, controles de acceso y metadatos) no solo cumpla con la Ley colombiana, sino que también integre o proponga la actualización de las reglas internas existentes.
- Fundamento de la gobernanza: Las conclusiones de este análisis serán la base para el diseño formal del Modelo de Gobernanza Documental, garantizando que las nuevas políticas del SGDEA estén alineadas con la estructura jerárquica y legal de la entidad.

5.2. Identificar brechas y riesgos

Se detectan las ineficiencias operativas y los cuellos de botella que impactan directamente en la productividad y la calidad del servicio al ciudadano. Esto incluye el análisis de la duplicidad documental y la existencia de silos de información entre dependencias, lo cual obstaculiza la toma de decisiones y la interoperabilidad institucional. La identificación de procesos manuales o lentos (como la búsqueda de documentos o la gestión de correspondencia) es clave para establecer los Indicadores Clave de Desempeño (KPIs) a mejorar con la automatización de los *workflows*.

- Problemas operativos y disfuncionalidades: Se detectan las ineficiencias operativas y los cuellos de botella que impactan directamente en la productividad y la calidad del servicio al ciudadano. Esto incluye el análisis de la duplicidad documental y la existencia de silos de información entre

dependencias, lo cual obstaculiza la toma de decisiones y la interoperabilidad institucional. La identificación de procesos manuales o lentos (como la búsqueda de documentos o la gestión de correspondencia) es clave para establecer los Indicadores Clave de Desempeño (KPIs) a mejorar con la automatización de los *workflows*.

- Riesgos críticos (legales, probatorios y reputacionales): Se analiza y categoriza la exposición actual de la Alcaldía a riesgos de alto impacto, incluyendo: Riesgo Probatorio, la pérdida de documentos críticos por fallos tecnológicos, deterioro de soportes o errores humanos, que compromete la defensa jurídica de la entidad; Riesgo de Integridad, la alteración malintencionada o accidental de documentos con valor legal, y la imposibilidad de demostrar la cadena de custodia de la información, esencial para procesos judiciales o disciplinarios; Riesgo de Continuidad del Negocio, la vulnerabilidad ante eventos de desastre que podrían detener la operación y la falta de Planes de Recuperación ante Desastres (DRP) efectivos; Riesgo Reputacional y de Privacidad, la ocurrencia de fugas de información confidencial o sensible, que impactan la privacidad de los ciudadanos y la imagen de la Alcaldía.

- Brechas normativas, archivísticas y técnicas: Se realiza una comparación exhaustiva del estado actual del *Universo Documental* y los procesos frente a los requisitos legales tales como Brechas de Cumplimiento Legal, donde se documentan las desviaciones frente a la normativa archivística colombiana (Ley 594, AGN) y las disposiciones de la Ley de Protección de Datos Personales (Ley 1581 de 2012). También brechas de preservación, donde Se identifica la falta de políticas de preservación a largo plazo (modelo OAIS) y el uso de formatos no aptos para la conservación digital (diferentes a PDF/A). Por último, tenemos Brechas de Seguridad Técnica que evalúa la insuficiencia de los controles de acceso, cifrado, y políticas de *backup* frente a los estándares de seguridad internacional, como la familia ISO/IEC 27001, asegurando que el diseño del SGDEA subsane estas deficiencias.

5.3. Establecer los cimientos del proyecto

Esta etapa final de la fase de Diagnóstico y Análisis es la transición formal de la teoría a la acción, traduciendo las brechas, los riesgos y la información levantada en requisitos precisos y en una hoja de ruta priorizada para las fases subsiguientes de diseño, selección tecnológica e implementación.

5.3.1 Requerimientos Detallados

Se procede a la definición detallada y verificable de los requisitos que el SGDEA debe cumplir obligatoriamente para la Alcaldía de Cartagena. Estos se dividen en:

- Requerimientos Funcionales: Se derivan directamente del análisis de los procesos (*to-be*). Estos definen qué debe hacer el sistema para modelar y automatizar el ciclo de vida documental (captura, gestión, retención, disposición final), asegurar la correcta aplicación de las TRD y facilitar la interoperabilidad con sistemas críticos (SIGEP, SECOP).

- Requerimientos No Funcionales: Definen cómo debe operar el sistema para ser sostenible y seguro. Incluyen especificaciones rigurosas sobre el rendimiento (tiempos de respuesta y concurrencia), la seguridad (controles de acceso, cifrado, registro de auditoría, alineación con ISO/IEC 27001), la usabilidad, la escalabilidad futura (volumetría proyectada) y la resiliencia (alta disponibilidad y DRP).

5.3.2. Priorización de la Implementación

El proyecto adoptará un enfoque de implementación progresivo y controlado, por lo cual se deben establecer criterios claros de priorización. El objetivo es definir qué procesos, dependencias o tipos documentales se abordarán en las primeras fases del proyecto para generar valor temprano (Quick Wins) y mitigar riesgos críticos. La priorización se fundamentará en:

- El impacto normativo y legal (ej. priorizar procesos de contratación y gestión de trámites críticos).
- La viabilidad técnica y la complejidad de la implementación (ej. iniciar con dependencias que tienen menor resistencia al cambio).
- El potencial de mejora de la eficiencia (KPIs) y la reducción del riesgo probatorio

Resumen del Sistema de Gestión Documental Electrónica de Archivo (SGDEA)

Componente Clave	Función Estratégica	Controles Asociados	Riesgo Mitigado
Pliego de Condiciones Técnico (PCT)	Documento rector que formaliza todos los requerimientos técnicos, funcionales y legales.	TCO (Costo Total de Propiedad), Criterios de Selección/Desarrollo (COTS o Medida).	Adquisición de solución incompatible o legalmente inviable; Desviaciones presupuestarias.
Módulo de Radicación (VUE)	Puerta de entrada única y controlada para la producción y captura de documentos electrónicos.	Asignación de NUR (Número Único de Radicación); Captura de Metadatos Obligatorios; Digitalización Certificada.	Pérdida de la cadena de custodia inicial; Falta de valor probatorio desde el origen.
Módulo Gestión y Trámite	Automatización del movimiento y uso de documentos dentro de la Alcaldía.	Modelado de Workflows Misionales; Aplicación estricta del Modelo RBAC; Motor de Plazos (alertas escalonadas).	Mora en la respuesta a trámites; Ineficiencia operativa; Acceso indebido a información sensible.

Componente Clave	Función Estratégica	Controles Asociados	Riesgo Mitigado
Integridad y Autenticidad	Garantiza la inalterabilidad del documento y su valor probatorio a lo largo del tiempo.	Sellos de Tiempo (Timestamping); Firmas Digitales/Electrónicas; Verificación Criptográfica (Hashes SHA-256).	Alteración o fraude documental; Pérdida de la fe pública; No repudio.
Clasificación y Organización	Estructura lógica del acervo documental y control archivístico.	Uso obligatorio del CCD (Cuadro de Clasificación Documental); Creación y control de Expedientes Electrónicos de Gestión (EEG).	Desorganización documental; Dificultad en la recuperación de la información.
Cumplimiento de TRD	Ejecución automatizada del ciclo de vida y el destino final de los documentos.	Motor de Retención Ineludible; Procedimiento de Eliminación Blindado (Acta inalterable y multi-aprobación); Alertas de Transferencia.	Incumplimiento de la normativa AGN; Retención innecesaria de documentos; Riesgo legal por eliminación indebida.
Trazabilidad y Seguridad	Seguimiento detallado de todas las acciones sobre los documentos.	Pista de Auditoría Forense Inmutable (registro de usuario, acción, tiempo, IP); Modelo RBAC (Control de Acceso Basado en Roles).	Fraude interno; Falta de evidencia para procesos judiciales/disciplinarios; Incumplimiento de la Ley 1581.
Interoperabilidad	Comunicación fluida y segura con otros sistemas gubernamentales.	Uso obligatorio de APIs RESTful; Integración con SIGEP y SECOP; Envío de datos a Portales de Transparencia.	Duplicidad de la información; Aislamiento tecnológico; Burocracia en trámites inter-institucionales.

Componente Clave	Función Estratégica	Controles Asociados	Riesgo Mitigado
Preservación a L/P	Garantía de la longevidad, legibilidad y acceso al patrimonio documental.	Conversión automática a Formatos Abiertos y Estándar (PDF/A); Alineación con el Modelo OAIS (Archivo Abierto).	Obsolescencia tecnológica; Imposibilidad de acceso a documentos históricos futuros.
Administración y Monitoreo	Gestión autónoma, flexible y orientación a la mejora continua.	Parametrización de TRD/CCD; Herramientas de diseño Low-Code para Workflows; Dashboard de KPIs (Objetivo 4.7); Doble Factor de Autenticación (2FA).	Dependencia de proveedores externos; Rigidez del sistema; Falta de control sobre la calidad del servicio.

6. Diseño, Selección y Desarrollo del SGDEA

Esta fase estratégica se inicia una vez que los requerimientos funcionales, no funcionales y el análisis de viabilidad (Costo Total de Propiedad - TCO) han sido rigurosamente definidos y validados en la etapa de diagnóstico. Al entrar en esta fase con cimientos sólidos y un Pliego de Condiciones Técnico (PCT) vinculante, la Alcaldía minimiza drásticamente el riesgo de desviaciones presupuestarias, fallos funcionales y obsolescencia tecnológica. Su propósito es trasladar la visión estratégica y los objetivos de cumplimiento en una solución tecnológica tangible, segura y sostenible, lista para ser implementada en la Alcaldía Mayor de Cartagena de Indias, garantizando que la inversión responda directamente a las brechas normativas y operativas críticas identificadas y que el sistema sea capaz de escalar conforme a las proyecciones de crecimiento.

6.1 Pliego de Condiciones Técnico (PCT) y Criterios de Selección

El Pliego de Condiciones Técnico (PCT) es el documento rector, vinculante y de obligatoria observancia que consolida y formaliza la totalidad de los

requerimientos funcionales, no funcionales y de interoperabilidad derivados del exhaustivo diagnóstico y el análisis de riesgos y TCO. Este instrumento se funda como la base innegociable para la Selección o Construcción de la Solución Tecnológica, asegurando que cualquier plataforma evaluada (COTS, *software* libre o desarrollo a medida) cumpla estrictamente con el mandato estratégico de la Alcaldía. Su propósito primordial es mitigar el riesgo de forma proactiva, impidiendo la adquisición de una solución que sea funcionalmente incompatible con los procesos críticos, que no cumpla con el marco legal archivístico colombiano (AGN) o que resulte tecnológicamente insostenible a largo plazo debido a la falta de escalabilidad o un TCO elevado.

Los criterios de selección final se ponderarán rigurosamente, priorizando la alineación normativa y el TCO:

- **Criterios del PCT:** Cumplimiento Archivístico Riguroso: La solución debe soportar la automatización total y el control ineludible del ciclo de vida documental, desde la captura hasta la transferencia y la disposición final, con la aplicación automatizada e irrestricta de las Tablas de Retención Documental (TRD), cumpliendo con la normativa del AGN en cada fase; Garantía de Integridad y Trazabilidad que exige la implementación de controles de integridad inmutable para sostener el valor probatorio del documento. Esto incluye la incorporación de Sellos de Tiempo (*Timestamping*) y Firmas Digitales para asegurar la autoría y el momento exacto de la aprobación, junto con un Registro de Auditoría Forense que capture de manera detallada e inalterable cada evento sobre el documento; Interoperabilidad Estratégica**,** donde el sistema debe proveer de forma obligatoria el uso de APIs RESTful robustas y bien documentadas, junto con la adhesión a protocolos de autenticación segura (ej. OAuth2), para garantizar la interoperabilidad bidireccional, eficiente y segura con el ecosistema tecnológico externo de la Alcaldía (SIGEP, SECOP) y las plataformas ciudadanas; por último, Resiliencia y Seguridad donde exigir el cumplimiento de los Requerimientos No Funcionales de Alta Disponibilidad y Resiliencia, y la implementación de controles de seguridad alineados con ISO/IEC 27001, mitigando el riesgo de incidentes y fallas de continuidad del negocio (DRP).

- **Viabilidad (TCO):** El Costo Total de Propiedad (TCO) se establece como el criterio financiero más decisivo y estratégico en la fase de selección, trascendiendo la simple comparación de precios de adquisición. Su análisis debe ser exhaustivo y cubrir un horizonte de proyección a mediano y largo plazo (ej. 5 a 7 años). El TCO debe incluir obligatoriamente los costos directos de licenciamiento e infraestructura, así como los costos indirectos de mantenimiento evolutivo, soporte técnico especializado, actualizaciones mayores, personalización profunda y capacitación continua del Capital Humano. Este análisis es fundamental para garantizar la sostenibilidad financiera del proyecto y la continuidad del SGDEA, asegurando que la solución sea capaz de absorber el crecimiento proyectado de la volumetría sin generar gastos inesperados por obsolescencia o licenciamiento adicional, mitigando el riesgo de parálisis operacional futuro.

6.2 Diseño Funcional y Técnico del SGDEA

En esta etapa crítica, se culmina la transición del análisis estratégico a la ingeniería detallada y la especificación del sistema. El objetivo es traducir el mandato formal de los Requerimientos del Pliego de Condiciones Técnico (PCT) —que define el "qué" es obligatorio, innegociable y normativo— en un "cómo" tangible, específico y blueprint. Esto implica la elaboración del plano arquitectónico y funcional de la solución a implementar o construir, asegurando que el diseño final no solo cumpla con la normativa archivística y la funcionalidad (el "qué" funcional), sino que también garantice la sostenibilidad técnica, la seguridad (alineación ISO/IEC 27001) y la escalabilidad de la plataforma tecnológica (el "cómo" no funcional). Este diseño servirá como el manual de instrucciones definitivo para la fase de desarrollo o selección del proveedor. Que debe estar soportado con:

6.2.1. Arquitectura Funcional y Módulos.

La definición de la Arquitectura Funcional constituye la estructura lógica del SGDEA, asegurando que el diseño de los módulos soporte la totalidad del ciclo de vida documental y los requerimientos de cumplimiento y seguridad. Los

Principales Módulos (Soporte al Ciclo de Vida) se diseñarán para que garanticen la operación eficiente y el control archivístico en cada fase**:**

- **Módulo de Radicación** (Ventanilla Única con Autenticación Segura): Punto de entrada y salida obligatorio de toda la documentación (física y electrónica), asegurando la inalterabilidad de la fecha de creación y la autenticación segura del usuario o ciudadano, fundamental para la trazabilidad inicial.

- **Módulo de Gestión y Trámite:** El núcleo operacional que soporta la automatización de los *workflows* misionales aprobados en el diseño, permitiendo la asignación, el seguimiento de plazos (control de mora) y la aplicación de acciones documentales (ej. firmas, anexos).

- **Módulo de Archivo (Central e Histórico):** Diseñado para aplicar la transferencia documental y la disposición final (eliminación o conservación permanente) de forma automatizada, garantizando la aplicación rigurosa de las TRD y el cumplimiento con los lineamientos del AGN.

- **Módulo de Administración del Sistema:** Permite la gestión de usuarios, roles, permisos y la parametrización autónoma de la estructura documental (CCD y TRD), facilitando la gobernanza continua del SGDEA.

6.2.2. Componentes Transversales (Valor Probatorio y Eficiencia)

Se definen las funcionalidades obligatorias que garantizan el valor legal de los documentos y la eficiencia operativa:

- **Digitalización Certificada:** Componente esencial para la conversión de documentos físicos con valor probatorio, asegurando que el proceso cumpla con los estándares técnicos y legales para la destrucción del soporte original, cuando sea aplicable.

- **Soporte para Firma Electrónica/Digital y Sellos de Tiempo:** Mecanismos criptográficos para asegurar la autoría, el consentimiento y la inalterabilidad de los documentos, mitigando el riesgo probatorio.

- **Motor de Búsqueda Avanzado**: Funcionalidad crítica que debe permitir la búsqueda precisa y segura por metadatos, contenido textual (Full-Text Search), y filtros de clasificación, aplicando siempre el control de acceso del usuario para garantizar la accesibilidad controlada.

- **Gestor de Reportes y KPIs:** Módulo para la generación de informes de gestión, auditoría y los Indicadores Clave de Desempeño (KPIs), crucial para la toma de decisiones gerenciales y la rendición de cuentas.

6.2.3. Modelo de Datos y Clasificación

Esta subsección define la estructura semántica, la longevidad y los requisitos de rendimiento críticos del SGDEA, asegurando que la solución sea tan robusta en su ingeniería como en su cumplimiento archivístico.

- **Modelo de Datos y Clasificación Archivística.** Se estructura la columna vertebral semántica del sistema, fundamental para el control archivístico y el valor probatorio.

  - **Estructuración de Reglas de Catalogación:** Implementación obligatoria de las reglas de catalogación y clasificación basadas en el Cuadro de Clasificación Documental (CCD) aprobado, asegurando que cada documento se posicione correctamente dentro de la estructura orgánica y funcional de la Alcaldía.

  - **Diseño de Metadatos Obligatorios:** Definición estricta de los esquemas de metadatos (administrativos, descriptivos, técnicos y de preservación) que deben ser capturados y gestionados por el sistema. Estos metadatos son el insumo esencial para garantizar la autenticidad,

integridad y el valor probatorio del documento electrónico, además de asegurar la interoperabilidad semántica con otros sistemas.

- **Preservación a Largo Plazo y Formatos.** Se establecen los requisitos para garantizar la pervivencia del patrimonio documental de La Heroica:

    - **Formatos Abiertos y Estándar:** Se especifica la obligación de privilegiar y gestionar formatos de archivo abiertos, estandarizados y reconocidos internacionalmente (ej. PDF/A).

    - **Alineación con OAIS:** La estrategia de almacenamiento y conservación debe ser diseñada en estricta conformidad con el Modelo de Referencia para un Sistema de Información de Archivo Abierto (OAIS), asegurando la gestión activa de la obsolescencia tecnológica y la accesibilidad futura de los documentos con valor histórico.

- **Consideraciones Estratégicas Clave.** Se definen los requisitos transversales que aseguran la resiliencia y la orientación al servicio del sistema:
    - **Trazabilidad Total e Inmutable:** El diseño debe garantizar la trazabilidad completa y forense de cada documento y cada acción de usuario, registrando el historial detallado de la cadena de custodia, lo cual es vital para la defensa jurídica de la entidad.

    - **Escalabilidad y Rendimiento:** La arquitectura debe diseñarse para la Escalabilidad inmediata y futura, capaz de gestionar el alto volumen proyectado de documentos y concurrencia de usuarios sin comprometer el rendimiento (*throughput*) del sistema, vinculándose al análisis de TCO y la proyección de volumetría.

    - **Interacción con la Ciudadanía:** El SGDEA debe ser capaz de integrarse con los Portales de Transparencia y sistemas de Peticiones, Quejas, Reclamos y Sugerencias (PQRS), facilitando la rendición de cuentas proactiva y la calidad del servicio ofrecido a la comunidad de Cartagena.

6.3. Desarrollo o Selección de la Solución

Con los diseños funcionales y técnicos aprobados, formalizados y vinculantes en el Pliego de Condiciones Técnico (PCT), la Alcaldía evaluará las alternativas disponibles para materializar el SGDEA. Esta etapa se convierte en la selección de la tecnología o la ejecución del desarrollo, garantizando que el camino elegido cumpla con las especificaciones técnicas y legales requeridas y se alinee con la estrategia de TCO y sostenibilidad proyectada.

Esta fase crítica se asegura de que la solución final responda directamente a la necesidad de blindaje normativo y eficiencia operativa identificada en el diagnóstico. La elección entre adquirir o desarrollar a medida debe basarse en una matriz de decisión objetiva y ponderada:

- **Adquisición de solución (COTS o *Software* Libre).** La evaluación de soluciones preexistentes (Comerciales [*Commercial Off-The-Shelf* - COTS] o de *Software* Libre) debe ser un proceso de *due diligence* riguroso y estratégico. Se priorizarán aquellas soluciones que demuestren una implementación probada y exitosa en el sector público colombiano, validando su capacidad para operar dentro del complejo ecosistema normativo nacional. Esto implica:

    - **Alineación Archivística Ineludible:** La solución debe demostrar una experiencia funcional y certificada en el manejo e integración del marco normativo del Archivo General de la Nación (AGN), incluyendo la parametrización de las TRD/TVD, la gestión de la tabla de retención y la disposición final, mitigando el riesgo legal.

    - **Interoperabilidad Nacional:** Es un requisito obligatorio que la plataforma cuente con mecanismos de integración funcionales y estables con los sistemas nacionales de gestión pública (ej. SIGEP, SECOP I/II, y sistemas de PQRSD), garantizando la articulación plena de la Alcaldía con el Gobierno Digital.

- **Sostenibilidad y Adaptabilidad:** Además del cumplimiento funcional, se evaluará la Hoja de Ruta de desarrollo del producto y la capacidad de la solución para ser personalizada para flujos de trabajo específicos de la Alcaldía de Cartagena (sin requerir código fuente ni licencias excesivas) y su viabilidad a largo plazo en términos de soporte técnico y TCO.

- **Desarrollo Interno o a Medida.** La opción de Desarrollo Interno o a Medida se activa si, tras la evaluación, ninguna solución preexistente (COTS o *Software* Libre) cumple a cabalidad con los requerimientos críticos del Pliego de Condiciones Técnico (PCT) o si el análisis de Costo Total de Propiedad (TCO) justifica una construcción propia. En este escenario, se exige un mandato arquitectónico que asegure la viabilidad técnica y la sostenibilidad a largo plazo:

  - **Arquitectura Tecnológica Modular y Sostenible:** Se exigirá el uso de una arquitectura moderna, modular y sostenible (ej. microservicios), esencial para la escalabilidad del sistema ante el crecimiento proyectado de la volumetría. Esta arquitectura debe facilitar la interoperabilidad mediante servicios definidos, aislando los componentes archivísticos para asegurar su integridad.

  - **Seguridad Integral (DevSecOps):** Se obliga la adopción de un Ciclo de Desarrollo Seguro (DevSecOps), garantizando que la seguridad y la protección de datos personales sean un componente integral y no un accesorio. El proceso de desarrollo incluirá la definición estricta del Stack Tecnológico y un ciclo de pruebas rigurosas que cubran rendimiento, usabilidad y obligatoriamente, pruebas de seguridad especializadas (hacking ético), asegurando la calidad del código y la mitigación de riesgos de integridad y accesibilidad.

  - **Soporte Técnico:** El Stack tecnológico elegido debe ser fácilmente mantenible por el equipo de TI de la Alcaldía o por un tercero especializado, para controlar el TCO y garantizar la continuidad del negocio.

En cualquier escenario, el resultado final debe ser una plataforma que satisfaga los umbrales de integridad, accesibilidad, trazabilidad y rendimiento definidos en el PCT.

6.3.1. Requisitos de Infraestructura, Respaldo y Continuidad del Negocio

- Modelo de Despliegue (On-premise/Cloud/Híbrido): Definición del modelo de *hosting* más adecuado según el análisis de TCO, la seguridad y la legislación colombiana (ej. Ley 1712 de Transparencia).

- Alta Disponibilidad y Resiliencia (DRP/BCP): Exigencia de un diseño de infraestructura que garantice la Alta Disponibilidad (HA) y la definición explícita de un Plan de Recuperación ante Desastres (DRP) y un Plan de Continuidad del Negocio (BCP) para el SGDEA, incluyendo la replicación en sitio alterno y la definición de RTO (Tiempo Objetivo de Recuperación) y RPO (Punto Objetivo de Recuperación).

- Almacenamiento WORM para Archivo Histórico: Especificación del tipo de almacenamiento requerido para los documentos de conservación total, garantizando la inmutabilidad de los archivos a nivel físico (WORM - *Write Once, Read Many*).

6.4 Controles de Integridad, Accesibilidad y Trazabilidad

Esta sección es fundamental para el blindaje jurídico y tecnológico del SGDEA. La correcta Selección o Desarrollo de la Solución debe garantizar que la plataforma incorpore, desde su concepción, pilares de control ineludibles que aseguren la confiabilidad, autenticidad e integridad del documento electrónico a lo largo de todo su ciclo de vida. Estos controles no son opcionales, sino mandatos normativos derivados de la necesidad de mitigar los riesgos probatorios, de privacidad (Ley 1581) y de suplantación identificados en el diagnóstico. El sistema debe, por diseño, garantizar la cadena de custodia

inmutable, transformando el documento electrónico en una evidencia legalmente defendible.

- Integridad (Garantía de no alteración). El control de Integridad constituye el mandato ineludible para sostener el valor probatorio y la fiabilidad jurídica del documento electrónico, mitigando activamente el riesgo de alteración o fraude. Se exige la implementación obligatoria y auditable de mecanismos criptográficos en puntos clave del ciclo de vida documental:

    - Autenticación y Tiempo Cierto: Implementación obligatoria de Firmas Electrónicas o Digitales para verificar la autoría y el consentimiento, complementada con Sellos de Tiempo (Timestamping) que aseguran cronológica e inalterablemente el momento exacto de la creación, aprobación o cualquier acción crítica sobre el documento.

    - Verificación Criptográfica: El sistema debe generar y almacenar Verificación Criptográfica (hashes como SHA-256) para cada documento. Este hash funciona como una huella digital inmutable que permite a la Alcaldía auditar y detectar cualquier modificación no autorizada o accidental posterior, garantizando el principio de no repudio.

    - Almacenamiento Seguro: Para un blindaje completo, se requiere el uso de repositorios de contenido controlado (WORM lógico o físico) que separen y protejan el binario del documento de los metadatos, asegurando que el contenido original permanezca intacto.

- Accesibilidad (Garantía de acceso controlado). El control de Accesibilidad es fundamental para la seguridad de la información y el cumplimiento de la Ley 1581 de 2012 (Protección de Datos Personales), mitigando activamente el riesgo de accesos indebidos o fugas de información:

    - Modelo de Permisos Riguroso (RBAC): Se exige la implementación estricta de un Modelo de Control de Acceso Basado en Roles (*Role-Based Access Control* - RBAC). Este modelo debe gestionar permisos de manera granular no por usuario individual, sino basados en los roles,

perfiles funcionales y dependencias definidas en la estructura orgánica de la Alcaldía.

- Segregación de Funciones y Privacidad: La aplicación del RBAC debe garantizar la segregación de funciones (Separation of Duties), limitando el acceso a documentos sensibles solo al personal autorizado y únicamente en el contexto de sus tareas. Esto asegura el cumplimiento de los principios de confidencialidad y acceso restringido de la Ley 1581.

- Búsqueda Segura y Filtrada: El motor de búsqueda avanzado, aunque potente (Full-Text Search), debe aplicar siempre y automáticamente los filtros de seguridad y permisos del usuario consultante. De esta manera, se garantiza que los funcionarios y ciudadanos solo visualicen aquellos documentos a los que tienen derecho legal y funcional, blindando el sistema contra la exposición no autorizada.

- Integración con Directorio Activo: Para la eficiencia y la seguridad de la gestión de identidades, el sistema debe ser capaz de integrarse con el Directorio Activo o servicios de gestión de identidad institucional de la Alcaldía, facilitando el control centralizado de las cuentas de usuario.

- Trazabilidad (Garantía de auditoría completa): El control de Trazabilidad es un imperativo legal y técnico que garantiza la cadena de custodia inmutable del documento, esencial para la rendición de cuentas y la defensa jurídica de la Alcaldía.

  - Pista de Auditoría Forense Inmutable: El SGDEA tiene el mandato de registrar una Pista de Auditoría (*Audit Trail*) que debe ser inmutable, detallada y cronológica. Esta pista debe capturar todos los eventos relevantes que ocurran sobre un documento, incluyendo su creación, la modificación de metadatos, la firma, cada consulta (quién y cuándo accedió), las transferencias de custodia y la disposición final (eliminación o conservación).

- Componentes del Registro: Cada registro de auditoría debe incluir, como mínimo, la siguiente información para garantizar su valor forense: qué usuario (identificador único), qué acción (ej. "consultar metadatos", "firmar"), cuándo (sello de tiempo preciso), desde dónde (dirección IP) y el resultado de la acción.
- Herramientas de Control: Se requiere un Módulo de Consulta y Reporting de Auditoría dedicado, accesible únicamente por las áreas de Control Interno, Archivo y TI autorizadas. Este módulo debe permitir la generación de informes detallados y la exportación de los datos para análisis, cumpliendo con la necesidad de verificación y vigilancia ciudadana establecida en el objetivo de Transparencia.

El éxito de la implementación dependerá directamente de que estos tres pilares se mantengan robustos y en equilibrio, garantizando que la Alcaldía Mayor de Cartagena mitigue de forma proactiva los riesgos de fraude, incumplimiento de privacidad y pérdida de la cadena de custodia, cumpliendo con su mandato de transparencia y resguardando el patrimonio documental a perpetuidad.

6.5 Requisitos de la interfaz administrativa

El módulo de administración es el "cerebro," el centro de gobernanza y la palanca de autonomía operativa del SGDEA. Está diseñado bajo el principio fundamental de minimizar la dependencia externa y potenciar las capacidades internas. Su función primordial es empoderar a los administradores autorizados (Archiveros, Tecnólogos y Auditores de Control Interno) para que puedan realizar una gestión autónoma, segura, parametrizable y flexible del sistema. De esta manera, se garantiza que la Alcaldía pueda responder con agilidad a los cambios normativos y a la evolución de sus procesos misionales, manteniendo el control total sobre la estructura documental (CCD y TRD) y las políticas de seguridad.

6.5.1. Funcionalidades estratégicas y de gobernanza

La interfaz debe ser una herramienta poderosa para el cumplimiento y la gestión del cambio:

- Parametrización Archivística Centralizada: Esta funcionalidad es la garantía de cumplimiento archivístico continuo del SGDEA. La interfaz de administración debe permitir de manera intuitiva, segura y auditable la Parametrización, actualización y gestión completa del ciclo de vida de las Tablas de Retención Documental (TRD) y el Cuadro de Clasificación Documental (CCD) directamente en el sistema, sin necesidad de recurrir a programación compleja.

  El objetivo es asegurar que la normativa interna (TRD/CCD) se aplique de forma inmediata, homogénea y automática en todos los *workflows* documentales, mitigando el riesgo de retenciones incorrectas o disposiciones finales no autorizadas. Esta capacidad de gestión interna es esencial para la autonomía operativa del área de archivo y la adaptación ágil del sistema a futuros cambios en la estructura orgánica o la normativa del Archivo General de la Nación (AGN).

- Configuración de *Workflows*: La interfaz de administración debe incorporar un motor de *workflows* robusto que opere bajo un principio de "configuración, no programación". Se exigirá la provisión de herramientas de diseño visual o *Low-Code* para la configuración ágil y modificación continua de los flujos de trabajo documentales, eliminando la dependencia de código complejo. Esta capacidad es crucial para:

  - Agilidad Operativa: Facilitar la adaptación inmediata del sistema a los cambios evolutivos en los procesos misionales y de apoyo de la Alcaldía.

  - Gobernanza Integrada: Asegurar que cualquier *workflow* configurado aplique automáticamente los controles de las Tablas de Retención Documental (TRD) y las reglas del Cuadro de Clasificación Documental (CCD), manteniendo el cumplimiento normativo en todo momento.

  - Mejora Continua: Permitir a los administradores internos optimizar los flujos de trabajo en función de los datos de desempeño recopilados en el Módulo de Monitoreo, impulsando el modelo de mejora continua.

- Definición de Políticas de Seguridad: Este es un control crítico e innegociable que se alinea directamente con el objetivo de seguridad y mitigación de riesgos de accesibilidad e integridad identificado en el diagnóstico. Es imprescindible que la interfaz de administración provea las herramientas para la definición, aplicación y monitoreo centralizado de políticas de seguridad robustas, asegurando el cumplimiento de estándares internacionales (ISO/IEC 27001) y la protección de datos personales (Ley 1581).

    - Control de Acceso Reforzado: Debe permitir la gestión detallada de la complejidad, caducidad y reutilización de contraseñas, y la implementación obligatoria del Doble Factor de Autenticación (2FA) para administradores y potencialmente, para usuarios clave.

    - Trazabilidad de Seguridad: La configuración de las políticas debe estar vinculada directamente al Registro de Auditoría Forense para asegurar la trazabilidad de cualquier cambio en los permisos o reglas de acceso.

    - Gestión de Sesiones: Incluir funcionalidades para la gestión de sesiones inactivas y el bloqueo automático de cuentas ante intentos fallidos, fortaleciendo la defensa contra ataques de fuerza bruta y accesos indebidos.

  Esta funcionalidad garantiza que la Alcaldía mantenga una postura de seguridad proactiva y adaptable frente a la evolución de las amenazas.

- Gestión de Usuarios y RBAC: La gestión de usuarios y permisos en el SGDEA no es solo una tarea administrativa, sino un control de seguridad y gobernanza esencial para la implementación del Modelo RBAC (Control de Acceso Basado en Roles).

    - Alineación Estricta y Automatizada: La interfaz debe facilitar la gestión integral del ciclo de vida de usuarios (alta, modificación, baja), roles y grupos de permisos. Es un requisito ineludible que esta gestión mantenga una alineación estricta y dinámica con el Modelo RBAC y la estructura orgánica de la entidad (dependencias, cargos y perfiles funcionales).

- Cumplimiento de Ley 1581: Este control es crítico para el cumplimiento de la Ley 1581 de 2012 (Protección de Datos Personales), ya que asegura que los accesos a la información sensible estén limitados por la función del empleado (necesidad de conocer), aplicando el principio de segregación de funciones.

- Integración con Sistemas de Identidad: Debe soportar la integración con el Directorio Activo o la Solución de Identidad Institucional de la Alcaldía (ej. LDAP/Single Sign-On - SSO). Esto centraliza la autenticación, aumenta la seguridad y reduce el riesgo de errores en la gestión manual de credenciales y permisos, garantizando una trazabilidad de identidad clara en la Pista de Auditoría.

6.5.2. Monitoreo y Usabilidad (Mejora Continua)

Esta subsección cierra el ciclo de desarrollo e integra la fase de implementación y operación, reconociendo que la tecnología por sí sola no garantiza el éxito. Su definición es crucial para la sostenibilidad del sistema y la adopción efectiva por el Capital Humano. Al estar diseñados bajo el principio de la Mejora Continua, estos requisitos buscan transformar el SGDEA en una fuente de inteligencia operativa, asegurando que su rendimiento se mantenga óptimo y que los funcionarios utilicen el sistema correctamente, minimizando la resistencia al cambio y optimizando la inversión a largo plazo.

- Monitoreo Estratégico (*Dashboard*). El SGDEA debe estar diseñado para ser un motor de inteligencia institucional. Por ello, se exige que la interfaz de administración incorpore un panel de control (*dashboard*) intuitivo, visual y en tiempo real. Este *dashboard* es la herramienta esencial para el Modelo de Mejora Continua (Objetivo 4.7) y la toma de decisiones gerenciales, permitiendo:

  - Vigilancia de KPIs Clave: Monitorear los Indicadores Clave de Desempeño (KPIs), como el estado de los documentos en mora, las

tasas de creación, los cuellos de botella en los workflows y la eficiencia en la atención de trámites, facilitando la rendición de cuentas.

- Salud Operativa: Ofrecer métricas sobre el rendimiento del sistema, la salud de la infraestructura, el uso de almacenamiento y la gestión de backups, garantizando la alta disponibilidad y la capacidad de respuesta del sistema.

- Auditoría de Uso: Visualizar patrones de uso del sistema, facilitando la identificación de necesidades de capacitación diferenciada y asegurando la adopción tecnológica.

- Usabilidad y Soporte Integrado. Para minimizar la resistencia al cambio y garantizar la apropiación tecnológica por parte de los administradores y archiveros, el diseño de la interfaz debe enfocarse en la experiencia del usuario:

  - Diseño Intuitivo y Coherente: Se exige una interfaz que sea intuitiva, limpia y coherente con los estándares de usabilidad de la Alcaldía.

  - Soporte Contextual Integrado: La interfaz debe incorporar Soporte Integrado (tooltips, ayudas contextuales y acceso directo a manuales de usuario/administración), lo que facilita el aprendizaje y la resolución de dudas en el momento de la operación, reduciendo la dependencia del soporte técnico externo y acelerando la curva de aprendizaje del Capital Humano.

  - Eficiencia en la Tarea: La usabilidad no es un lujo, sino un requisito de eficiencia, asegurando que las tareas críticas de gestión documental y archivística se realicen de manera rápida, con un mínimo margen de error y sin generar duplicidades documentales.

6.5.3. Accesibilidad técnica

El SGDEA, como sistema transversal y orientado al servicio público, debe garantizar la Accesibilidad Técnica Universal para todos los usuarios internos y la

ciudadanía. Este requisito va más allá de la mera funcionalidad; es un mandato de eficiencia, usabilidad y transparencia, crucial para la adopción total del sistema por parte del Capital Humano y el cumplimiento del Objetivo Cívico.

- Compatibilidad Universal y Arquitectura Abierta: La plataforma debe ser completamente funcional y operable a través de navegadores web estándar y modernos, evitando la dependencia de tecnologías propietarias o *plugins* específicos. Esto asegura un acceso sin fricciones, facilita la interoperabilidad con sistemas externos y reduce los costos de licenciamiento y soporte a largo plazo (TCO).

- Diseño Adaptativo (*Responsive Design*): Es obligatorio implementar un diseño responsivo (o adaptativo) que garantice la usabilidad y la coherencia del UI/UX en cualquier dispositivo (ordenadores de escritorio, tabletas y móviles). Esta capacidad es fundamental para facilitar la supervisión y la realización de tareas administrativas básicas (ej. aprobación de flujos, consulta de KPIs) por parte del personal directivo y misional que opera en movilidad, promoviendo la agilidad operacional y la toma de decisiones oportuna.

El cumplimiento de estos requisitos asegura que la inversión en el SGDEA no solo sea una mejora tecnológica, sino una transformación integral de la gobernanza documental que posiciona a la Alcaldía en la vanguardia del Gobierno Digital colombiano.

6.6 Pruebas piloto e implantación gradual

El proceso de despliegue del SGDEA se abordará con una estrategia de alto control y bajo riesgo, descartando categóricamente la implementación de tipo "*big bang*" (adopción total e inmediata). Se optará por un enfoque controlado, incremental y progresivo, lo cual es un requisito esencial para garantizar la estabilidad del sistema y la adopción efectiva por parte del Capital Humano, cumpliendo directamente con el Objetivo 4.8 de Validación del proyecto.

6.6.1. Fase Piloto (Validación Crítica - UAT)

La fase piloto es la prueba de fuego del diseño y la validación final antes de la puesta en producción.

- Selección Estratégica: Se seleccionarán dependencias representativas que combinen procesos de mediana a alta complejidad con una alta disposición al cambio. Esta selección debe abarcar los tipos documentales más críticos para la Alcaldía, asegurando que se pruebe la rigurosidad del Modelo de Datos, TRD y *Workflows* en un contexto real.

- Entorno Controlado (UAT): La implementación se realizará en un entorno de Pruebas de Aceptación de Usuario (*User Acceptance Testing* - UAT) con datos de prueba o datos reales anonimizados.

- Ejecución y *Feedback*: El objetivo primario es ejecutar escenarios de uso cotidianos y extremos, simulando la volumetría y concurrencia reales. Se debe establecer un mecanismo formal de recopilación de *feedback* de los usuarios piloto, identificando puntos de fricción, fallos de usabilidad y desviaciones funcionales o normativas.

- Ajustes y Cierre: Se realizarán los ajustes necesarios en configuraciones, parametrización de flujos de trabajo, formularios y permisos. La fase solo se dará por concluida y aprobada cuando se demuestre que la solución cumple con el 95% de los requerimientos funcionales y no funcionales del PCT.

6.6.2. Plan de implantación gradual (Adopción Sostenible)

Una vez superada la fase piloto, se procede al despliegue masivo mediante un plan estructurado para gestionar la escala y el factor humano.

- Hoja de Ruta por Fases: Se diseñará una Hoja de Ruta de despliegue por fases, priorizando las dependencias según los criterios de impacto, riesgo

y complejidad definidos en la etapa 5.3. Cada fase debe tener objetivos de migración y adopción claros.

- Gestión del Cambio Integral. Cada fase de despliegue debe ir intrínsecamente acompañada por una estrategia de Gestión del Cambio (Change Management), que incluye:
    - Comunicación Proactiva y Sensibilización: Informar a la comunidad de usuarios sobre el valor del SGDEA y el impacto de las nuevas herramientas.
    - Capacitación Intensiva y Diferenciada: Ofrecer jornadas de Capacitación Intensiva adaptadas específicamente a los perfiles de usuario (radicadores, tramitadores, líderes de proceso, archiveros) para asegurar el uso correcto de las funcionalidades de Integridad, Accesibilidad y Trazabilidad.
- Soporte Reforzado (*Hypercare*): Durante las primeras semanas de operación en cada dependencia, se establecerá un plan de soporte de alta disponibilidad (*Hypercare*) para resolver incidencias de manera inmediata y guiar a los usuarios en la transición.

Este enfoque asegura la mitigación del riesgo de rechazo por parte del usuario y garantiza que la inversión tecnológica se traduzca en eficiencia real y cumplimiento normativo en toda la Alcaldía.

6.6.3. Estrategia de Migración y Saneamiento Documental

- Alcance de la Migración: Definición de qué acervo documental será migrado (Archivos Centrales/Históricos) y qué volúmenes se mantendrán en el archivo físico (por antigüedad o valoración).
- Saneamiento Pre-Migratorio: Requisito de saneamiento y valoración de los fondos documentales existentes antes de su ingesta al SGDEA, garantizando que solo se migre documentación válida y clasificada según la TRD/CCD aprobado.

- Migración de Metadatos: Establecimiento de protocolos para la migración de metadatos desde sistemas heredados, asegurando la coherencia semántica con el nuevo Modelo de Datos del SGDEA.

- Ingesta y Certificación: Modelado del proceso de ingesta masiva (ya sea por digitalización o transferencia electrónica), asegurando la aplicación de los controles de Integridad (Hashes) al momento de la carga para establecer la nueva Cadena de Custodia Electrónica.

6.7 Alineación del SGDEA con el Marco Normativo Colombiano

Esta matriz valida que cada componente del SGDEA responda directamente a un mandato legal o archivístico del país, fundamental para el blindaje jurídico del proyecto.

Componente Clave del SGDEA	Mandato Archivístico/Legal (Colombia)	Principio SGDEA Reforzado
Punto Único de Radicación (VUE)	Ley 594 de 2000 (Principio de Procedencia)	Autenticidad y Control de Origen.
Motor de Retención Documental	Decreto 1080 de 2015 (TRD/TVD); Acuerdo AGN 004/2019	Confiabilidad y Cumplimiento del Ciclo de Vida.
Uso de Firmas Digitales y Sellos de Tiempo	Ley 527 de 1999 (Mensaje de Datos); Ley 962 de 2005	Integridad del Contenido y No Repudio.
Modelo RBAC / Restricción de Acceso	Ley 1581 de 2012 (Protección de Datos Personales)	Accesibilidad (Controlada) y Confidencialidad.
Pista de Auditoría Forense Inmutable	Decreto 1080 de 2015 (Obligación de Trazabilidad)	Trazabilidad y Cadena de Custodia.
Conversión a PDF/A (Archivo Histórico)	Guías y Estándares de Preservación del AGN (Modelo OAIS)	Disponibilidad y Legibilidad a Largo Plazo.

Componente Clave del SGDEA	Mandato Archivístico/Legal (Colombia)	Principio SGDEA Reforzado
Integración con Sistemas Nacionales (SECOP/SIGEP)	Ley 1712 de 2014 (Transparencia); Ley de Gobierno Digital	Interoperabilidad y Transparencia.
Digitalización Certificada	Decreto 1080 de 2015; Reglamentación AGN	Confiabilidad y Valor Probatorio del documento digitalizado.

6.8 Conclusión de la Fase de Diseño y Selección

Los beneficios estratégicos para culminar de forma exitosa la fase de Diseño y Selección generará beneficios estratégicos inmediatos y a largo plazo para la Alcaldía Mayor de Cartagena:

Beneficio Estratégico	Impacto en la Alcaldía	Mitigación de Riesgos
Blindaje Jurídico y Probatorio	El sistema garantiza la cadena de custodia inmutable y el valor legal del documento electrónico (Art. 4.4).	Riesgo de pérdida probatoria y suplantación.
Autonomía Operativa	La interfaz de administración permite la gestión interna de las TRD, el CCD y los workflows, reduciendo drásticamente la dependencia y los costos de soporte de proveedores externos (TCO).	Riesgo de TCO elevado y obsolescencia funcional.
Cumplimiento Normativo Total	El diseño integra la normativa archivística (AGN) y la Ley de Protección de Datos (Ley 1581) desde la concepción del sistema.	Riesgo de multas por incumplimiento y fugas de datos.
Eficiencia y Escalabilidad	La arquitectura modular y la gestión de workflows automática optimizan los	Riesgo de cuellos de botella y parálisis operacional.

Beneficio Estratégico	Impacto en la Alcaldía	Mitigación de Riesgos
	procesos misionales y aseguran la capacidad de crecimiento del sistema.	
Transparencia y Rendición de Cuentas	El diseño del Módulo de Monitoreo (Dashboard) y la integración con portales ciudadanos facilitan la vigilancia y la respuesta ágil a los requerimientos de la ciudadanía.	Riesgo reputacional y de desconfianza cívica.

7. Modelado del ciclo documental y el diseño de flujos de trabajo

Una vez que los Requerimientos Formales y el Diseño Funcional y Técnico (Capítulo 6) han sido rigurosamente definidos y el Pliego de Condiciones Técnico (PCT) ha sido aprobado, la atención se centra en la ingeniería de procesos.

Este capítulo aborda la etapa crucial de traducción de los Procesos de Gestión Documental Archivística (POGDA) de la Alcaldía en modelos operacionales claros, eficientes y completamente automatizables. El objetivo es establecer el diseño lógico (Blueprint) de cómo el SGDEA aplicará la normativa archivística (TRD y CCD), los controles de integridad y el Modelo RBAC en la operación diaria. Este modelado es la base sobre la cual se configurarán los *Workflows* en el sistema, asegurando que la tecnología refuerce la legalidad, la eficiencia y la trazabilidad en cada etapa del ciclo de vida documental.

7.1 Modelado del Ciclo de Vida del Documento Electrónico

El diseño y la configuración del SGDEA deben basarse ineludiblemente en el Ciclo de Vida del Documento Electrónico (desde la planeación hasta la disposición final), conforme a las directrices del Archivo General de la Nación (AGN).

El modelado en esta fase asegura que el sistema asuma la responsabilidad automatizada de la custodia y el control, garantizando que cada etapa (planeación, producción, gestión, organización, transferencia, disposición y preservación) esté completamente regulada y auditada por la plataforma. Esto implica que el sistema no solo gestiona, sino que aplica activamente las reglas de autenticidad, integridad y trazabilidad definidas en el PCT (Capítulo 6), transformando la normativa archivística en flujos operativos.

A continuación, se da una descripción de las diferentes etapas:

Etapa	**Significado y Control en el SGDEA**
Planeación	Definición de Instrumentos: Corresponde a la etapa inicial donde se definen y aprueban los instrumentos que el SGDEA debe aplicar de manera obligatoria: el Cuadro de Clasificación Documental (CCD) y las Tablas de Retención Documental (TRD).
Producción	Creación y Captura Controlada: El sistema garantiza el registro oficial del documento (NUR), la asignación de los metadatos obligatorios y la aplicación de mecanismos de Integridad (ej. Sello de Tiempo y Firma Digital), asegurando el valor probatorio desde el origen.
Gestión	Uso y Trámite Operacional: Se refiere al movimiento y uso del documento dentro de la Alcaldía. El SGDEA automatiza esto a través de los Flujos de Trabajo (Workflows), aplicando el Modelo RBAC para el control de acceso y el Motor de Plazos para el control de mora.
Organización	Clasificación y Agrupación Lógica: El sistema clasifica el documento automáticamente según el CCD y crea los Expedientes Electrónicos de Gestión (EEG), agrupando la documentación relacionada a un mismo asunto para mantener la unidad archivística.

Etapa	Significado y Control en el SGDEA
Transferencia	Movimiento de Custodia: Es la transición de responsabilidad y acceso del documento, ya sea de forma primaria (del Archivo de Gestión al Archivo Central) o secundaria (del Archivo Central al Archivo Histórico). El SGDEA automatiza las alertas y el proceso de transferencia lógica.
Disposición	Destino Final (Eliminación o Conservación): El SGDEA ejecuta la decisión final dictada por la TRD una vez cumplido el tiempo de retención. La Eliminación se realiza bajo estricto control y la generación de un Acta de Eliminación inmutable; la Conservación Total prepara el documento para su valor histórico.
Preservación	Longevidad y Acceso Futuro: Aplicada a los documentos de valor histórico o permanente. El SGDEA realiza la conversión a Formatos de Preservación (ej. PDF/A) y aplica políticas de gestión de la obsolescencia tecnológica, en línea con el Modelo OAIS.

7.1.1. Etapa de Producción y Captura

Esta etapa es la más crítica para el blindaje jurídico del SGDEA, ya que define la calidad de auténtico documento electrónico desde el momento de su ingreso al sistema (nacimiento). El diseño debe garantizar que todo contenido pase por filtros de Integridad, Autenticidad y Trazabilidad desde el origen, en estricto cumplimiento del PCT (Capítulo 6).

- Punto Único de Radicación (Ventanilla Única Electrónica - VUE): Se establece la obligatoriedad de la Ventanilla Única Electrónica (VUE) como la única puerta de entrada y salida de toda la documentación oficial (tanto la generada internamente como la recibida externamente). El sistema debe asignar el Número Único de Radicación (NUR) de forma inalterable y secuencial, iniciando formalmente la cadena de custodia y eliminando la posibilidad de existencia de documentos sin control o "por fuera" del sistema.

- Asignación Inteligente de Metadatos y Clasificación: El sistema debe obligar la captura de los Metadatos Esenciales y de Preservación definidos en el diseño (Capítulo 6.2.3). De manera crítica, la interfaz debe facilitar la asignación automática o asistida de la Clasificación Documental (CCD) (Serie y Subserie) al momento de la radicación. Esta acción enlaza inmediatamente el documento con las reglas de retención de la TRD, definiendo su ubicación lógica y garantizando la interoperabilidad semántica.

- Aplicación Criptográfica de Valor Probatorio: Para asegurar la autenticidad, la integridad y el no repudio, el sistema debe aplicar automáticamente controles criptográficos:

    - Sellos de Tiempo (*Timestamping*): Asegurando cronológicamente el momento exacto del registro oficial.

    - Firmas Electrónicas/Digitales: Aplicables a la autoría o la aprobación del documento.

    - Verificación Criptográfica (*Hashes*): Generación y almacenamiento del *hash* (ej. SHA-256) del documento en el momento de la captura, lo que

constituye la huella digital inmutable para futuras auditorías de integridad.

- Digitalización Certificada: Para los documentos que se originan en soporte físico, se modela el proceso de Digitalización Certificada. El SGDEA debe garantizar que la imagen digital obtenida cumpla con los estándares técnicos y legales para adquirir valor probatorio equivalente al original, permitiendo, si es requerido por la TRD y la normativa del AGN, la disposición (destrucción) del soporte físico original bajo estricto control.

7.1.2. Etapa de Gestión y Trámite (Workflows)

Esta etapa constituye el corazón operativo del SGDEA, donde la eficiencia, la legalidad y la seguridad del manejo documental se ponen a prueba. El modelado de los flujos de trabajo debe transformar los procesos manuales en rutas automatizadas y controladas, garantizando que el documento cumpla su función administrativa de manera ágil y auditable.

- Modelado de Flujos Misionales y de Soporte: Se realizará la ingeniería de detalle de los Flujos de Trabajo (*Workflows*) para todos los procesos críticos identificados en el diagnóstico (ej. Contratación, PQRS, Resoluciones y Licencias), utilizando las herramientas de diseño visual del módulo de administración (Capítulo 6.5). Cada *workflow* debe reflejar con precisión las etapas de Inicio, Visto Bueno (VB), Aprobación, Revisión, Cierre y Distribución, tal como están definidas en el Manual de Procesos de la Alcaldía. El diseño debe incluir bifurcaciones y condiciones lógicas que permitan adaptar el flujo a la naturaleza específica de cada trámite.

- Aplicación Estricta del Modelo RBAC y Seguridad. La asignación de tareas, la capacidad de acceso o la potestad de firmar documentos dentro del flujo deben regirse estrictamente por el Modelo RBAC (*Role-Based Access Control*) (Capítulo 6.4). Esto garantiza la Segregación de Funciones y el principio de mínimo privilegio, asegurando que:

    - Solo los usuarios con el rol y perfil funcional adecuado puedan acceder, modificar o aprobar el documento.

- Se cumpla con el mandato de Protección de Datos Personales (Ley 1581), restringiendo el acceso a información sensible a quien "necesita conocer".

- Cada acción crítica (firma, aprobación) dentro del *workflow* se registre automáticamente en la Pista de Auditoría Forense (Capítulo 6.4).

- Control de Términos (Motor de Plazos y Alertas Críticas): El sistema debe incorporar un Motor de Plazos de alta precisión que ejecute un control riguroso sobre los términos legales. Este componente es esencial para la mitigación del riesgo de mora y el incumplimiento normativo en la atención a la ciudadanía y los procesos internos.

- Alertas Automatizadas: El motor debe calcular automáticamente el tiempo restante y generar alertas tempranas (escalonadas) a los responsables (incluyendo a sus superiores) cuando un documento o trámite se acerque a su fecha límite legal o interna.

- Trazabilidad del Tiempo: El sistema debe registrar en la auditoría el tiempo exacto que el documento permaneció en cada etapa del *workflow*, lo cual es una métrica clave de desempeño (KPI) para la Mejora Continua (Capítulo 6.5.1).

7.2. Diseño de la Organización y Disposición Documental

Esta sección define el modelado archivístico fundamental del SGDEA, crucial para la integridad, recuperación y cumplimiento legal de los documentos a largo plazo.

Se especifica detalladamente cómo el SGDEA debe:

- Organizar la información de manera lógica y jerárquica, utilizando el Cuadro de Clasificación Documental (CCD) como estructura ineludible.

- Aplicar de forma automatizada e ineludible las reglas de retención y disposición final (TRD).

El éxito de esta fase garantiza que el sistema no solo almacene documentos, sino que funcione como un archivo electrónico de gestión activo y legalmente conforme, facilitando la trazabilidad de la vida media y final de cada registro, desde el Archivo de Gestión hasta la Preservación Histórica.

7.2.1. Clasificación y Organización (CCD)

Esta sección asegura la aplicación funcional del principio de orden original y procedencia, elementos fundamentales del SGDEA para la recuperación efectiva y la aplicación de las reglas de retención.

- Jerarquía Automatizada y Vinculación Ineludible: El sistema debe usar el Cuadro de Clasificación Documental (CCD) aprobado como su estructura base y mapa lógico inmutable. La clave es la automatización: la correcta asignación de la Serie y Subserie documental durante la fase de radicación (7.1.1) debe determinar automáticamente y sin errores la ubicación jerárquica y lógica del documento dentro de la estructura orgánica y funcional de la Alcaldía. Esto elimina la discrecionalidad del usuario y garantiza la homogeneidad en la clasificación.

- Creación, Foliación y Cierre de Expedientes Electrónicos. Se debe modelar el proceso de gestión de Expedientes Electrónicos de Gestión (EEG), que son las unidades archivísticas fundamentales:

    - Unidad Archivística: El SGDEA debe asegurar que todos los documentos relacionados a un mismo asunto (ej. una resolución específica, un contrato, un proceso disciplinario) se agrupen y mantengan la unidad archivística a lo largo del tiempo.

    - Foliación Lógica y Controlada: El sistema debe gestionar la foliación de manera lógica, asignando un orden secuencial inalterable a los documentos dentro del EEG, lo cual es vital para su valor probatorio.

    - Cierre y Activación de la TRD: El modelo debe definir las condiciones bajo las cuales el EEG se declara cerrado (finalización del trámite), ya

que este evento crítico activa el Motor de Retención Documental para iniciar el conteo de los plazos de la TRD.

7.2.2. Aplicación y Cumplimiento de las TRD

Esta sección modela la automatización del destino final del documento, un proceso de alto riesgo legal que debe ser gestionado de forma ineludible por el SGDEA para garantizar la integridad del patrimonio documental y el cumplimiento de la normativa del AGN.

- Motor de Retención Ineludible: Se diseña el Motor de Retención, que se constituye como el componente de cumplimiento normativo central del SGDEA. Este motor debe aplicar de forma automática, ineludible y auditable los tiempos de retención definidos en las Tablas de Retención Documental (TRD). Es crucial que el motor inicie el conteo del tiempo de retención automáticamente al detectarse el evento de Cierre del Expediente Electrónico de Gestión (EEG), garantizando la precisión cronológica del plazo de vigencia administrativa.

- Transferencia y Disposición Final Controlada. El sistema debe gestionar activamente las transiciones de custodia y el destino final del documento, asegurando la trazabilidad de la decisión archivística:

    - Alertas de Transferencia: El Motor de Retención debe generar alertas tempranas y escalonadas a los administradores del sistema para iniciar la Transferencia Documental (lógica y de acceso) del Archivo de Gestión al Archivo Central, y posteriormente, la preparación para la Disposición Final.

    - Proceso de Eliminación Blindado: La función de Eliminación Documental, al ser una acción de riesgo máximo, solo debe poder ejecutarse bajo estrictos controles de seguridad y multi-aprobación (segregación de funciones), y siempre posterior a la verificación de la no existencia de procesos judiciales o administrativos pendientes. El sistema debe generar de forma automatizada e inalterable el Acta de

Eliminación, registrando el *hash* de los documentos eliminados y la evidencia de la destrucción lógica en la Pista de Auditoría Forense (Capítulo 6.4), manteniendo la Trazabilidad completa del proceso.

- Preparación para Conservación Total: En el caso de documentos con valor histórico (Conservación Total), el sistema debe disparar la conversión a formatos de preservación (PDF/A) y la transferencia al módulo de Archivo Histórico para la preservación a largo plazo.

7.3 Interoperabilidad y Preservación

Esta sección del modelado garantiza que el SGDEA sea un componente activo y comunicable dentro del ecosistema digital de la Alcaldía (Interoperabilidad) y que los documentos con valor histórico puedan ser legibles y accesibles a perpetuidad (Preservación).

- Integración de Servicios y APIs Estratégicas. Se define el modelado de los servicios de interoperabilidad (APIs RESTful) como un mandato de la solución (Capítulo 6.1). Estas interfaces son esenciales para:
  - Conexión Bidireccional: Asegurar la comunicación fluida y segura con los sistemas misionales y de apoyo críticos externos (ej. SECOP para la gestión contractual, SIGEP para información de funcionarios, sistemas PQRS).
  - Transparencia Activa: Permitir el envío automatizado y controlado de metadatos o copias de documentos públicos a los Portales de Transparencia de la Alcaldía.
  - Evitar la Duplicidad: La integración debe permitir que los sistemas externos consuman la información documental desde el SGDEA, convirtiéndolo en la fuente única de verdad (Single Source of Truth).

- Formatos y Conversión Obligatoria para Preservación: Para mitigar el riesgo de obsolescencia tecnológica, se establecen reglas estrictas:
  - Conversión Automatizada: Se modelan las reglas de conversión automática y controlada a Formatos de Preservación Abiertos y Estándar (ej. PDF/A,

XML). Esta conversión debe dispararse en el momento de la Transferencia al Archivo Histórico (Disposición Final), asegurando que el contenido binario del documento esté preparado para el largo plazo.

- Alineación con el Modelo OAIS: La estrategia de preservación está diseñada conforme al Modelo de Referencia para un Sistema de Información de Archivo Abierto (OAIS). Esto garantiza que el sistema esté preparado para gestionar la obsolescencia tecnológica (ej. migración de formatos futuros), el acceso continuo y la preservación de la información de forma auténtica y legible a largo plazo.

7.4 Controles de seguridad aplicados por evento crítico

Esta matriz detalla cómo los tres pilares de control (Integridad, Accesibilidad y Trazabilidad) definidos en el Capítulo 6.4 se activan de forma obligatoria en los momentos más sensibles del ciclo de vida documental. Es crucial para el equipo de Seguridad y Control Interno.

Evento Crítico del Documento	Control de Integridad Requerido	Control de Accesibilidad (RBAC) Requerido	Control de Trazabilidad Requerido
1. Radicación (Ingreso al VUE)	Aplicación de Sello de Tiempo y generación del Hash SHA-256 inicial.	Solo el rol de "Radicador Autorizado" puede generar el NUR.	Registro de la hora y el usuario que realiza la captura inicial.
2. Aprobación/Firma en Workflow	Aplicación de la Firma Digital/Electrónica para validar la identidad y el consentimiento.	Permiso de "Firma" restringido a los roles de "Directivo" o "Funcionario con Fe Pública".	Registro de la acción de firma (exitosa/fallida) y la validación de la identidad.

Evento Crítico del Documento	Control de Integridad Requerido	Control de Accesibilidad (RBAC) Requerido	Control de Trazabilidad Requerido
3. Consulta de Datos Sensibles	Verificación automática del Hash para asegurar que el documento no fue alterado desde su última acción.	Filtro de acceso automático del sistema basado en la Ley 1581 (solo usuarios con "Necesidad de Conocer").	Registro de la consulta (usuario, documento y hora exacta) en la Pista de Auditoría.
4. Eliminación de Documentos	Hash del documento final antes de la eliminación; generación del Acta de Eliminación (documento nuevo inmutable).	Requisito de Multi-Aprobación de roles (Archivo, TI y Control Interno) antes de la ejecución.	Registro del Acta de Eliminación y la evidencia de la destrucción lógica, asegurando la trazabilidad del fin de la custodia.
5. Cierre del Expediente (EEG)	N/A	El permiso para "Cerrar EEG" se restringe al rol de "Líder de Proceso" o "Jefe de Archivo de Gestión".	Registro de la fecha de cierre del EEG, evento que dispara el Motor de Retención.

8. Funcionalidades clave del SGDEA

Las funcionalidades clave del SGDEA para la Alcaldía se articulan como la materialización técnica y obligatoria de los principios archivísticos rectores: autenticidad, integridad, confiabilidad, disponibilidad y trazabilidad. Estas capacidades garantizan que el sistema trascienda la función de ser un simple repositorio de archivos, erigiéndose como una plataforma de gobernanza documental activa que preserva el valor probatorio, legal y patrimonial de los documentos electrónicos de la Alcaldía.

La base de estas funcionalidades se sustenta en el estricto cumplimiento del marco normativo colombiano (Ley 594 de 2000, Decreto 1080 de 2015) y los lineamientos ineludibles del Archivo General de la Nación (AGN), blindando a la Alcaldía contra riesgos legales y garantizando una gestión documental eficiente en el contexto del Gobierno Digital.

Síntesis de las Funcionalidades Clave:

Pilar Estratégico	Función Obligatoria	Fundamento Legal/Técnico
Control de Ingreso	Ventanilla Única Electrónica (VUE) y Radicación Única, con asignación de Metadatos Esenciales y clasificación automática (CCD).	Ley 594/00 (Principio de Procedencia)
Valor Probatorio	Aplicación automática de Sellos de Tiempo y gestión de Firmas Digitales/Electrónicas al momento de la creación/aprobación.	Ley 527/99 (Mensaje de Datos); Control de Integridad (SHA-256)
Gestión Operacional	Motor de Workflows (automatización de trámites) y Motor de Plazos (control de términos legales).	Eficiencia Administrativa; Mitigación de Riesgo de Mora
Cumplimiento Archivístico	Motor de Retención Documental para la aplicación ineludible de las TRD/TVD y la gestión de la disposición final.	Decreto 1080/15 (Reglamentación AGN)
Seguridad y Trazabilidad	Modelo RBAC para acceso controlado y Pista de Auditoría Forense inmutable.	Ley 1581/12 (Protección de Datos); Cadena de Custodia

Pilar Estratégico	Función Obligatoria	Fundamento Legal/Técnico
Sostenibilidad	Conversión a Formatos de Preservación (PDF/A) y estrategias alineadas al Modelo OAIS.	Preservación a Largo Plazo

Estos se agrupan en tres pilares estratégicos:

8.1 Almacenamiento seguro de documentos electrónicos

Este pilar es la garantía de la integridad y la disponibilidad física y lógica de la información. El SGDEA debe ir más allá del simple almacenamiento, implementando una arquitectura de repositorios que asegure que cada documento electrónico sea almacenado, gestionado y protegido de forma adecuada durante la totalidad de su ciclo de vida activo, semiactivo e histórico.

- Inviolabilidad del Contenido: La solución debe utilizar mecanismos de almacenamiento que garanticen la inviolabilidad del binario del documento. Para los documentos con valor a largo plazo o histórico, se exigirá el uso de repositorios con funcionalidad WORM (Write Once, Read Many) a nivel lógico o físico, previniendo cualquier alteración o eliminación accidental/maliciosa del registro original.
- Gestión de la Disponibilidad: El sistema debe integrarse con una estrategia de Alta Disponibilidad (HA) y respaldos automáticos, asegurando la accesibilidad constante al documento electrónico y cumpliendo con los RPO/RTO definidos en el Plan de Continuidad del Negocio (BCP) (referencia a la sección 6.3.3).
- Segregación y Control Ambiental: Los documentos deben almacenarse en repositorios lógicamente segregados según su etapa en el ciclo de vida (Gestión, Central, Histórico) y su sensibilidad (confidencialidad), aplicando controles de acceso específicos en el nivel del repositorio, además del Modelo RBAC a nivel funcional.

Este control asegura que la infraestructura de *storage* sea tan robusta como el marco normativo y la tecnología de gestión, sosteniendo el principio de confiabilidad del SGDEA.

8.1.1 Gestión centralizada y estructurada de repositorios

Esta sección define la arquitectura lógica de almacenamiento, asegurando que el diseño del SGDEA refleje fielmente la normativa archivística colombiana (AGN) y garantice la fiabilidad y recuperabilidad de los documentos. El objetivo es eliminar la dispersión de la información y asegurar que la estructura física y lógica del repositorio sea una manifestación directa de la autoridad archivística.

- Repositorio Único Lógico (*Single Source of Truth*):
  - Se exige la implementación de un Repositorio Único Lógico que opere como la Fuente Única de Verdad (*Single Source of Truth*) para toda la documentación de archivo de la Alcaldía.
  - Este repositorio puede estar compuesto por un conjunto de repositorios federados (ej. uno para Archivo de Gestión y otro para Preservación), pero su acceso y gestión deben estar centralizados y controlados por el SGDEA para evitar silos de información y duplicidad documental.
  - El diseño debe priorizar la separación física/lógica del documento binario de sus metadatos, optimizando la consulta de la información y reforzando la seguridad de los registros.

- Organización Archivística Jerárquica e Ineludible:
  - La estructura de almacenamiento (lógica y física) del repositorio debe reflejar fielmente, de manera jerárquica y obligatoria el Cuadro de Clasificación Documental (CCD) y las Tablas de Retención Documental (TRD) de la Alcaldía.
  - La organización se materializa en la creación y control de los Expedientes Electrónicos de Gestión (EEG). El sistema debe garantizar que cada

documento, al ser clasificado, sea insertado automáticamente en la Serie y Subserie documental correspondiente, manteniendo la unidad archivística y el principio de procedencia en todo momento.

- Esta estructura jerárquica es crítica porque es el mecanismo mediante el cual el SGDEA aplica las reglas de retención, transferencia y disposición final del Motor de Retención (Capítulo 7.2.2) al expediente completo y no solo al documento individual.

8.1.2. Soporte de múltiples formatos y políticas de normalización

Este punto aborda la gestión de la diversidad tecnológica y es crucial para la sostenibilidad y la preservación a largo plazo del acervo documental (Principio de Preservación). El SGDEA debe ser capaz de manejar cualquier formato documental que ingrese a la Alcaldía, pero debe aplicar una política de normalización rigurosa para aquellos que deben ser conservados.

- Gestión Nativa y Amplia de Formatos:
  - El sistema debe poseer la capacidad nativa y robusta para ingestar, indexar y gestionar una amplia gama de formatos de uso común y legalmente aceptados.
  - Esto incluye, pero no se limita a, formatos de ofimática (DOCX, ODT, XLSX), imagen (TIFF, JPG, PNG), formatos de contenido estático (PDF), correos electrónicos con sus adjuntos (EML, MSG) y de forma crítica, contenido multimedia (audio/video).
  - La gestión nativa debe asegurar que el contenido de texto de todos estos formatos sea indexado por el Motor de Búsqueda (Capítulo 6.2.1) para su recuperación eficiente (Full-Text Search).

- Conversión Obligatoria y Políticas de Preservación:
  - Para mitigar el riesgo de obsolescencia tecnológica y garantizar la legibilidad futura, el SGDEA debe incorporar políticas y herramientas de conversión automática o asistida a formatos estandarizados y abiertos.

- La conversión obligatoria es para el Formato de Preservación PDF/A (PDF/A-1, PDF/A-2 o PDF/A-3), el estándar internacional para la conservación a largo plazo de documentos textuales.
- Momento de la Conversión: Tal como se modeló en el Capítulo 7.3, esta conversión debe dispararse de forma obligatoria y controlada en el momento de la Transferencia al Archivo Histórico (Disposición Final), asegurando que se conserve el contenido de manera auténtica, legible e independiente del software original.
- Alineación AGN: Este proceso debe seguir estrictamente las guías y estándares definidos por el Archivo General de la Nación (AGN) para la preservación digital.

8.1.3. Seguridad en reposo, en tránsito y en uso:

La seguridad del SGDEA se concibe bajo un modelo de defensa en profundidad, asegurando que la protección de los documentos electrónicos no dependa únicamente del control de acceso (RBAC), sino que esté garantizada en cada fase de su ciclo tecnológico: cuando están almacenados, cuando se mueven a través de la red y cuando están siendo utilizados. Este es un requisito ineludible para la Certificación ISO/IEC 27001 y el cumplimiento del mandato de confidencialidad de la Ley 1581.

- Cifrado en Reposo (At-Rest) - Protección del Almacenamiento:
  - El cifrado de los datos en reposo es obligatorio. El almacenamiento físico o lógico donde residen los documentos de la Alcaldía debe estar criptográficamente protegido mediante algoritmos robustos y actualizados (ej. AES-256).
  - Este cifrado debe aplicarse a nivel de disco, volumen o a nivel de base de datos (o repositorio de objetos), para proteger la información incluso en caso de acceso físico o lógico no autorizado al servidor o en caso de robo de infraestructura de almacenamiento.

- La gestión de las claves de cifrado debe realizarse de forma segura y separada del repositorio de documentos (ej. mediante un HSM o KMS institucional).

- Cifrado en Tránsito (In-Transit) - Protección de la Comunicación:

  - Toda comunicación entre los navegadores de los usuarios, las aplicaciones cliente y los servidores del SGDEA debe ser obligatoriamente cifrada de punto a punto.
  - Se exige el uso de protocolos seguros y actualizados como HTTPS/TLS 1.2 o superior, con certificados digitales válidos y de confianza, para prevenir ataques de intercepción y sniffing (man-in-the-middle).
  - Esta obligatoriedad se extiende a todas las interfaces de Interoperabilidad (APIs) definidas en el Capítulo 7.3, asegurando que la comunicación entre sistemas críticos se mantenga igualmente blindada.

- Seguridad Aplicativa (In-Use) y Controles Multicapa:

  - La seguridad debe operar en múltiples capas para garantizar la defensa en profundidad. Esto incluye controles de acceso a nivel de sistema operativo y base de datos, pero fundamentalmente en la lógica de la aplicación (Capas 6 y 7 del modelo OSI).
  - El diseño de la aplicación debe adherirse a las mejores prácticas de seguridad de software (ej. OWASP Top 10), previniendo vulnerabilidades como inyección SQL, Cross-Site Scripting (XSS) y fallas en el control de acceso.
  - Es crítico que los controles del Modelo RBAC (Capítulo 6.4) se ejecuten en la capa de la aplicación, validando que el usuario tenga el permiso exacto para realizar la acción solicitada (Principio de Mínimo Privilegio).

8.1.4. Control de acceso y confidencialidad (Modelo RBAC):

Este componente es la realización funcional de la Ley 1581 (Protección de Datos) y la Ley 1712 (Transparencia) dentro del SGDEA. El control de acceso no es una característica opcional, sino el mecanismo de blindaje que asegura la confidencialidad y el principio de mínimo privilegio, garantizando que la información sensible solo sea accesible por quienes tienen una función legítima para consultarla.

- Permisos Granulares y Principio de Mínimo Privilegio:
    - El sistema debe operar bajo un estricto Modelo de Control de Acceso Basado en Roles (*Role-Based Access Control* - RBAC), permitiendo la definición de permisos extremadamente detallados (granulares) aplicados a las acciones críticas sobre el documento (crear, leer, modificar, eliminar, firmar) y sobre el expediente (cerrar, transferir).
    - El diseño debe obligar la aplicación del Principio de Mínimo Privilegio, donde los usuarios solo reciben los permisos estrictamente necesarios para cumplir con su labor en un *workflow* específico, fortaleciendo la seguridad interna y la segregación de funciones.

- **Vinculación Orgánico-Funcional y Gestión del Ciclo de Vida del Usuario:**
    - Los roles y permisos deben estar dinámicamente asociados a la estructura orgánica, las dependencias y los cargos de la Alcaldía.
    - Se exige la capacidad de integración con el sistema de identidad institucional (ej. Directorio Activo/LDAP o SSO) para automatizar el ciclo de vida del usuario (alta, cambio de rol, baja) y asegurar que el cambio de cargo o el retiro implique la revocación inmediata de los privilegios de acceso, minimizando el riesgo residual.

- **Gestión de Información Clasificada y Control de Confidencialidad:**

    - El SGDEA debe incorporar un Control de Confidencialidad mediante la aplicación de marcadores de seguridad (etiquetas) que permitan gestionar documentos con reserva legal o que son clasificados (datos personales o de seguridad).

    - El sistema debe aplicar automáticamente la restricción de acceso según el marcador (Ley 1712 de 2014) y de manera crítica, gestionar y notificar la fecha de expiración de la reserva, momento en el cual el documento debe ser desclasificado y pasar a ser de acceso público, garantizando el cumplimiento de los tiempos de la Ley de Transparencia.

8.1.5. Gestión de versiones y trazabilidad de cambios

Este punto asegura la Integridad y Trazabilidad de los documentos que, por su naturaleza administrativa (ej. borradores, informes en revisión, resoluciones en proceso), deben ser modificados antes de su aprobación final. La gestión de versiones es el mecanismo que preserva la integridad forense del documento a través de su evolución, garantizando que el historial completo y el valor probatorio de cada estado intermedio se mantenga inalterado.

- Versión Automática.

    - El sistema debe implementar la creación automática e ineludible de una nueva versión cada vez que un documento es modificado, guardado o editado por un usuario con permisos de modificación (RBAC).

    - El SGDEA no debe sobrescribir el archivo original. En su lugar, debe preservar el *hash* criptográfico y el binario de cada versión anterior como un registro inmutable, asegurando que el historial de producción del documento esté completamente disponible para auditorías.

- Esto es obligatorio para mantener la Cadena de Custodia de los documentos dinámicos hasta su cierre final.

- Historial de Cambios. La funcionalidad debe ir más allá de la simple numeración de versiones. El sistema debe proveer una visualización clara del historial de cambios que indique con nivel forense:
  - ¿Quién? (Identidad del usuario, alineado con el SSO/LDAP).
  - ¿Qué? (Metadatos modificados y opcionalmente, las diferencias textuales entre versiones).
  - ¿Cuándo? (Sello de Tiempo exacto de la modificación).

Toda esta información debe ser registrada en la Pista de Auditoría Forense como parte del registro de eventos del documento.

- Recuperación Controlada: Posibilidad de recuperar versiones anteriores, siendo esta acción debidamente registrada en la pista de auditoría.
  - El SGDEA debe permitir la recuperación controlada (*Rollback*) de cualquier versión anterior del documento para restaurarla como la versión activa.
  - Control Crítico: Esta acción de recuperación debe estar restringida por el Modelo RBAC a roles con altos privilegios (ej. Administrador de Archivo o TI), y la acción de *Rollback* debe ser registrada de manera prioritaria y detallada en la Pista de Auditoría, justificando la necesidad de la recuperación.

8.1.6 Gestión de expedientes híbridos y control de bodegas físicas

El SGDEA debe ofrecer una gestión unificada que abarque tanto el entorno digital como el físico, garantizando la trazabilidad integral de los Expedientes Híbridos.

- Vínculo Indisociable: El sistema debe mantener un vínculo indisociable entre la versión electrónica de un expediente y su contraparte física (carpeta o caja), utilizando identificadores únicos (ej. códigos de barras o QR) para el acceso y la trazabilidad.

- Módulo de Control de Bodegas: El SGDEA debe integrar un Módulo de Control de Bodegas (similar a un WMS) para gestionar la ubicación exacta (*ubicación topográfica*), el préstamo, la consulta física y el cronograma de Disposición Final de los soportes físicos de los documentos con valor temporal.

- Automatización de Transferencias: La plataforma debe automatizar los procedimientos de Transferencia Documental Primaria y Secundaria (Física), generando los listados de control y las actas requeridas por la normativa, basadas en el Motor de Retención (8.3.1).

8.2 Interoperabilidad con el ecosistema Institucional

El SGDEA no puede operar como una isla tecnológica. Su valor estratégico se multiplica al integrarse de manera fluida, segura y auditable con el resto de los sistemas de información misionales y de apoyo de la Alcaldía, consolidando un ecosistema digital coherente y alineado con los principios de Gobierno Digital.

Este pilar funcional garantiza que el SGDEA sea reconocido y tratado como la Fuente Única de Verdad (*Single Source of Truth* - SSOT) para toda la información documental y archivística de la entidad.

8.2.1. Arquitectura orientada a servicios (APIs):

La arquitectura del SGDEA debe ser concebida como un "Hub" de servicios documentales dentro de la Alcaldía. Esto requiere una arquitectura intrínsecamente orientada a servicios que permita que el sistema interactúe no solo como consumidor, sino como proveedor de funciones documentales para el resto del ecosistema.

- APIs Estándar: El sistema debe exponer un conjunto de APIs REST/JSON bien documentadas y seguras, que permitan a otros sistemas realizar operaciones como:
    - El sistema debe exponer un conjunto completo y modular de APIs (Interfaz de Programación de Aplicaciones) que sigan los estándares modernos REST/JSON.
    - La documentación de estas APIs (ej. usando OpenAPI/Swagger) debe ser clara, exhaustiva y técnica, facilitando la integración por parte de terceros y de los equipos de TI de la Alcaldía.
    - Es un requisito de seguridad que todas las APIs operen con autenticación robusta (ej. *tokens* OAuth2) y cifrado de tránsito (TLS 1.2+) para proteger la transferencia de metadatos y documentos.

8.2.2. Integración con sistemas gubernamentales y misionales clave

Esta sección del diseño garantiza que el SGDEA sea un facilitador activo de la política de Gobierno Abierto y Digital, trascendiendo el uso administrativo interno para convertirse en un mecanismo de cumplimiento de la Ley de Transparencia (Ley 1712 de 2014) y en un punto de interacción eficiente con la ciudadanía.

Integración con Portales de Transparencia:

- El SGDEA debe ser capaz de alimentar de manera automática y controlada los Portales de Transparencia y Acceso a la Información Pública (PQRSD).

- Esta integración se realizará mediante APIs que permitan el envío seguro y programado de copias digitales y metadatos de los documentos de naturaleza pública, garantizando que la publicación sea oportuna y cumpla con los estándares de información mínima exigida por la ley.

- Es fundamental que el sistema respete los marcadores de reserva legal (Capítulo 8.1.4) y solo publique aquellos documentos que hayan superado su período de reserva o que sean intrínsecamente públicos.

Soporte a la Interacción Ciudadana (PQRSD):

- El SGDEA debe integrarse bidireccionalmente con los sistemas de Peticiones, Quejas, Reclamos, Sugerencias y Denuncias (PQRSD).

- Entrada: La radicación de un PQRS en el sistema ciudadano debe disparar automáticamente la radicación oficial del documento en el SGDEA (generación del NUR) y el inicio del *workflow* de trámite correspondiente (Capítulo 7.1.2).

- Salida: La respuesta oficial generada y firmada digitalmente dentro del SGDEA debe ser transferida automáticamente al sistema de PQRSD para ser notificada al ciudadano, cerrando el ciclo de manera eficiente y legal.

Replicación de Metadatos para Consulta Pública:

- Para optimizar el rendimiento de la consulta ciudadana, el SGDEA debe poder replicar un subconjunto de metadatos no sensibles a una base de datos pública o de consulta rápida, permitiendo que el ciudadano realice búsquedas y seguimientos (ej. por número de radicación o asunto) sin impactar directamente la infraestructura transaccional del archivo central.

Este enfoque asegura que el SGDEA sea un motor de rendición de cuentas y servicio público, alineado con la misión de la Alcaldía de promover un Gobierno Digital abierto y accesible.

8.2.3. Interoperabilidad semántica y técnica:

La interoperabilidad no se limita a la simple conexión física de sistemas mediante APIs (Interoperabilidad Técnica); exige que los datos intercambiados posean un significado coherente y unívoco (Interoperabilidad Semántica). Este requisito es vital para mantener la integridad de los metadatos y asegurar que la información generada o consumida por el SGDEA sea fiable y legalmente válida en cualquier sistema de la Alcaldía.

Vocabularios Controlados y Autoridad Archivística:

- El SGDEA debe ser el repositorio maestro que impone el uso de vocabularios controlados y catálogos de referencia a todos los sistemas interconectados.

- Los catálogos críticos incluyen: el Cuadro de Clasificación Documental (CCD), las Series/Subseries (para la tipología documental), los Códigos de Dependencias (Estructura Orgánica) y los Estados de Trámite (Flujos de Trabajo).

- El sistema debe obligar a que cualquier *input* (a través de APIs o UI) utilice estos vocabularios predefinidos, eliminando ambigüedades y asegurando que todos los sistemas "hablen el mismo idioma" archivístico.

Mapeo Riguroso de Metadatos y Consistencia:

- El SGDEA debe facilitar las herramientas para realizar el mapeo obligatorio y auditable de metadatos entre los identificadores internos del SGDEA y los identificadores de los sistemas externos (ej. mapear el ID de un contrato del SECOP con el NUR del SGDEA).

- Este mapeo es crucial para garantizar la consistencia y la integridad referencial de la información. Por ejemplo, si un sistema de gestión contractual envía un documento final, el SGDEA debe poder traducir los metadatos adjuntos para clasificarlos correctamente según el CCD y aplicar la TRD correspondiente.

- El sistema debe rechazar transacciones vía API si los metadatos obligatorios (ej. clasificación) no cumplen con los estándares y valores definidos en los vocabularios controlados.

Uso de Esquemas de Intercambio Estándar:

- Para la Interoperabilidad Técnica, se exige el uso de esquemas de datos estandarizados (ej. esquemas XML o JSON bien definidos) para estructurar el intercambio de documentos y metadatos. Esto asegura la fiabilidad del proceso de transferencia y permite una fácil validación automática de la estructura de la información, fortaleciendo el control de Integridad en Tránsito.

8.2.4. Orquestación de flujos de trabajo inter-sistémicos:

La orquestación de flujos es la capacidad de que el SGDEA se convierta en el controlador lógico (Orquestador) de procesos que abarcan múltiples aplicaciones. Esto trasciende el workflow interno (Capítulo 7.1.2) para automatizar procesos de negocio complejos, garantizando que el ciclo de vida del documento continúe incluso cuando la acción se produce en un sistema externo (ej. financiero, presupuestal o contractual).

Automatización Basada en Eventos (Event-Driven Architecture):

- El SGDEA debe integrarse mediante un modelo de Arquitectura Orientada a Eventos (*Event-Driven Architecture*) que permita la automatización de procesos inter-sistémicos sin intervención manual.

- Disparadores Clave: Eventos críticos en sistemas externos (ej. la liquidación financiera de un contrato en el ERP, la aprobación final de una licencia en el sistema misional o el cierre de un proceso disciplinario) deben funcionar como disparadores remotos de acciones en el SGDEA.

- Ejemplo Crítico: El cierre de un contrato en el sistema financiero debe disparar automáticamente la acción de Cierre del Expediente Electrónico de Gestión (EEG) en el SGDEA, lo cual, a su vez, activa el Motor de Retención Documental para iniciar el conteo de los plazos de la TRD.

Notificaciones Cruzadas y *Webhooks*:

- El SGDEA debe habilitar mecanismos de notificación activa (*push*), como Webhooks, para alertar a otros sistemas de que un evento documental crítico ha ocurrido.

- Cadena de Eventos: Por ejemplo, la firma digital de una resolución en el SGDEA (evento de salida) debe notificar al Portal de Transparencia para su publicación inmediata o al sistema de Nómina para que continúe con el proceso de pago asociado, asegurando la coherencia operacional y la inmediatez.

Monitorización y Resiliencia de la Orquestación:

- El sistema debe contar con un módulo de monitorización de la orquestación que rastree la ejecución de estas transacciones de múltiples pasos.

- Se exige que el SGDEA sea resiliente, es decir, que si un sistema externo falla temporalmente al recibir un *webhook* o al consultar una API, el SGDEA implemente mecanismos de reintento o de registro de errores para garantizar que la transacción se complete o sea registrada para su revisión manual, manteniendo la integridad del proceso de negocio.

8.2.5. Inteligencia artificial y automatización de la ingesta

El SGDEA debe integrar módulos de Inteligencia Artificial (IA) y Aprendizaje Automático (*Machine Learning*) para optimizar la ingesta y la clasificación documental, minimizando la intervención humana y el error.

- Clasificación Automática y Metadata Extraction: El sistema debe ser capaz de procesar documentos escaneados o electrónicos, aplicar Reconocimiento Óptico de Caracteres (OCR) avanzado, y utilizar modelos de IA para clasificar automáticamente el documento dentro del Cuadro de Clasificación Documental (CCD) y extraer los metadatos clave (ej. fecha, remitente, asunto del trámite) con una precisión documentada superior al 90%.

- Validación Semántica: La IA debe validar la congruencia de los metadatos extraídos contra las reglas del CCD y los tipos documentales, alertando sobre posibles errores de clasificación antes de la radicación final.

- Encaminamiento Inteligente (*Smart Routing*): Basado en el contenido y la clasificación automática, el SGDEA debe poder pre-asignar el documento al proceso o dependencia responsable (*workflow*), acelerando el inicio de los trámites.

8.2.6. Integración NATIVA con plataformas BPM empresariales

El SGDEA debe actuar como el repositorio de registro y evidencia de todos los procesos ejecutados en plataformas de Gestión de Procesos de Negocio (BPM).

- Conectores Nativos: Se exige la disponibilidad de conectores nativos o APIs especializadas para la integración bidireccional con plataformas BPM de uso común en el sector público, permitiendo:

    - Inicio de Procesos: La radicación de un documento en el SGDEA debe poder iniciar automáticamente un proceso o *workflow* en la plataforma BPM.

- Evidencia Documental: La plataforma BPM debe poder almacenar la evidencia documental (actas, informes, decisiones) directamente en el Expediente Electrónico del SGDEA al finalizar una tarea o un proceso, asegurando que la evidencia esté completa y con la firma digital asociada.

- Sincronización de Metadatos: La integración debe asegurar la sincronización de metadatos clave (identificadores, estados del proceso) entre ambos sistemas para garantizar la trazabilidad de la auditoría.

8.3 Gestión del patrimonio digital y preservación a largo plazo

Esta funcionalidad se erige como el mecanismo de blindaje contra la obsolescencia tecnológica y es la máxima garantía de que la memoria institucional y el patrimonio documental de la Alcaldía trasciendan el tiempo. El SGDEA asegura que los documentos electrónicos que, según la TRD, tienen Valor Histórico o Conservación Total, se mantengan auténticos, íntegros, fiables y accesibles a perpetuidad, en estricto cumplimiento del mandato del Archivo General de la Nación (AGN). La estrategia de preservación está intrínsecamente diseñada bajo el Modelo de Referencia para un Sistema de Información de Archivo Abierto (OAIS), lo que implica la capacidad de gestionar la ingesta de Paquetes de Información, la conversión obligatoria a formatos de preservación (ej. PDF/A) y la monitorización de la obsolescencia tecnológica para realizar futuras migraciones controladas, asegurando así la continuidad de la memoria institucional.

8.3.1. Aplicación de tiempos de retención y valoración documental:

Esta funcionalidad es la ejecución automatizada de la autoridad archivística delegada en las Tablas de Retención Documental (TRD) y es crítica para la preservación de la memoria institucional y la limpieza de los archivos (eliminación legal de lo innecesario).

Identificación y Aplicación Automática Ineludible:

- El Motor de Retención (Capítulo 7.2.2) debe aplicar automáticamente los tiempos de retención definidos en las TRD y las Tablas de Valoración Documental (TVD) a los Expedientes Electrónicos de Gestión (EEG), una vez que el expediente ha sido formalmente cerrado.

- El sistema debe identificar, de forma programada y sin intervención manual, aquellos expedientes que han cumplido su vigencia administrativa y legal en el Archivo de Gestión y Central, clasificando su destino final entre Conservación Total (Valor Permanente) y Eliminación.
- Es imprescindible que el sistema realice la doble verificación de no tener procesos judiciales o fiscales abiertos antes de proceder con cualquier cambio de disposición.

Marcado, Transferencia Lógica y Preparación para Preservación:

- Una vez cumplido el tiempo de retención en las fases de gestión y central, el sistema debe generar alertas a los roles archivísticos (RBAC) para la Transferencia Documental Lógica de estos expedientes al Archivo Histórico.

- Los expedientes marcados para Conservación Total deben ser preparados automáticamente para la preservación, disparando el proceso de conversión a formatos PDF/A (Capítulo 8.3) y la generación de los Paquetes de Información de Archivo (AIP) requeridos por el Modelo OAIS antes de su ingreso definitivo al módulo de preservación.

- El sistema debe generar la documentación archivística asociada (ej. Actas de Transferencia) de forma automática y con garantía de inalterabilidad.

8.3.2. Metadatos de preservación (PREMIS):

Los metadatos de preservación son la prueba forense digital que garantiza que un documento histórico mantenga su autenticidad y fiabilidad a pesar de los cambios tecnológicos y la migración de formatos. La gestión de estos metadatos debe adherirse al estándar internacional PREMIS (Preservation Metadata Implementation Strategies), reconocido por el AGN y el Modelo OAIS.

Registro Técnico Detallado e Inmutable (Esquema PREMIS):

- El SGDEA debe ser capaz de capturar, gestionar y conservar un conjunto enriquecido de metadatos de preservación que van más allá de los metadatos descriptivos administrativos. Estos datos deben registrarse en el momento de la ingesta al Archivo Histórico y mantenerse inmutables, vinculados al objeto digital (documento binario):
    - Información del Objeto Digital: Detalle técnico del archivo, incluyendo el formato, tamaño, Checksum (Hash), codificación de caracteres, y la aplicación (*software* y *hardware*) utilizada para su creación.
    - Eventos de Preservación: Un registro completo y cronológico de cada acción de preservación (migración de formato, validación de integridad, cambio de soporte de almacenamiento o aplicación de nuevos algoritmos de cifrado).
    - Derechos y Procedencia: Historial detallado de la cadena de custodia (quién lo tuvo, cuándo y con qué autoridad) y los derechos de acceso y uso asociados al documento a lo largo del tiempo.

Contexto Archivístico Indisociable:

- Estos metadatos técnicos de preservación deben permanecer indisociablemente vinculados a los metadatos descriptivos y administrativos (CCD, Serie, Subserie) del documento.
- Esta vinculación es esencial para garantizar no solo la autenticidad (el documento no ha sido alterado), sino también la comprensión del contexto y el significado del documento en el futuro, incluso cuando las estructuras organizacionales o las aplicaciones tecnológicas de la Alcaldía hayan cambiado.

El uso del esquema PREMIS asegura que el SGDEA esté preparado para generar los Paquetes de Información de Archivo (AIP) requeridos para la preservación a largo plazo, fortaleciendo el cumplimiento del Modelo OAIS.

8.4. Estrategias activas de preservación digital:

La preservación digital no es un evento estático, sino un proceso continuo y activo que requiere la intervención planificada del SGDEA para anticiparse a la obsolescencia. Esta funcionalidad asegura que el sistema esté preparado para los desafíos tecnológicos a largo plazo, manteniendo la legibilidad y la autenticidad de los documentos históricos.

Vigilancia Tecnológica, Planificación y Ejecución de Migración:

- El SGDEA debe incorporar un módulo de Vigilancia Tecnológica que monitoree activamente los formatos de archivo utilizados y los estándares de preservación (ej. nuevas versiones de PDF/A, cambios en los formatos de uso masivo).

- Al detectar un riesgo inminente de obsolescencia, el sistema debe permitir la planificación y ejecución controlada de Estrategias de Migración. Por ejemplo, el sistema debe gestionar la transferencia masiva de documentos de un formato antiguo a un estándar más reciente (ej. de PDF/A-1 a PDF/A-3).

- Control Forense: Cada migración debe ser ejecutada bajo estricto control, registrando el evento en los Metadatos de Preservación (PREMIS), y generando la verificación de integridad (hash) del nuevo archivo, garantizando que el contenido intelectual permanezca inalterado.

Normalización de Formatos (Video, Audio e Imagen):

- La estrategia de normalización debe extenderse a todos los tipos de formatos sensibles a la obsolescencia que maneje la Alcaldía (ej. minutas de reuniones, evidencia audiovisual, planos CAD).

- El sistema debe incluir herramientas y perfiles para convertir y normalizar formatos de video, audio o imagen a estándares abiertos, sostenibles y de alta compresión sin pérdida de información (lossless), antes de su ingreso al Archivo Histórico. Esto puede incluir estándares como TIFF para imágenes, o formatos abiertos para audio y video definidos en las guías del AGN.

Modelo de Replicación Geográfica y Resiliencia:

- Como parte de la estrategia de preservación activa (alineada al DRP del Capítulo 6.3.3), el SGDEA debe garantizar la replicación geográfica de los paquetes de información de archivo (AIP) en sitios alternos o en la nube institucional. Esto previene la pérdida de la información histórica debido a fallas físicas localizadas o desastres, cumpliendo con el principio de disponibilidad a largo plazo.

8.5. Repositorios de preservación confiables:

Este componente aborda la gestión de la infraestructura física y lógica que sustenta el Archivo Histórico, asegurando la durabilidad, inmutabilidad y disponibilidad física de los documentos con valor permanente. Un repositorio confiable es el pilar tecnológico que soporta la estrategia de preservación a largo plazo del SGDEA.

Almacenamiento de Alta Durabilidad y Resiliencia Geográfica:

- Se exige la utilización de tecnologías de almacenamiento diseñadas explícitamente para la retención a largo plazo y la alta durabilidad, como

repositorios de objetos o soluciones de almacenamiento archivístico que ofrezcan una durabilidad extrema

- El sistema debe implementar obligatoriamente la replicación geográfica activa de los Paquetes de Información de Archivo (AIP) en diferentes ubicaciones físicas y/o lógicas (sitio principal, sitio alterno y posiblemente, almacenamiento en la nube institucional) para mitigar el riesgo de pérdida total debido a desastres naturales, fallas de *hardware* masivas o ataques cibernéticos localizados (alineación con el DRP del Capítulo 6.3.3).

Verificación Periódica de Integridad y Detección de Corrupción de Datos (*Bit Rot*):

- La pasividad en el almacenamiento es un riesgo. El sistema debe ejecutar procesos programados de Verificación Periódica de Integridad (*Fixity Check*).

- Estos procesos deben recalcular el *hash* criptográfico (checksum) de los documentos almacenados y compararlo con el hash original registrado en los Metadatos de Preservación (PREMIS).

- Sistema de Alerta: La funcionalidad debe ser capaz de detectar y alertar automáticamente a los administradores sobre cualquier corrupción de datos (*bit rot*) o alteración inesperada del archivo binario. Al detectar la corrupción, el sistema debe disparar procedimientos de recuperación automática desde la copia replicada geográficamente, asegurando la autosanación de los repositorios.

Tecnología WORM y Control de Retención:

- El repositorio debe soportar tecnologías WORM (Write Once, Read Many) a nivel lógico, físico o mediante la configuración de políticas de retención inmutables en el almacenamiento de objetos. Esto asegura que, una vez que el documento es transferido y marcado para conservación total, no pueda ser modificado ni borrado antes de la fecha final (si aplica) o por error humano.

8.6. Acceso y difusión del patrimonio documental

Esta funcionalidad culmina el ciclo de vida documental y de preservación, transformando el Archivo Histórico de un repositorio pasivo en un centro de consulta activo y un recurso de Transparencia para la sociedad. El objetivo es maximizar el valor del patrimonio digital, garantizando la disponibilidad y el acceso controlado a la memoria institucional.

Diagrama del Modelo OAIS:

Portal de Consulta Histórica y *Discovery*:

- El SGDEA debe ofrecer un módulo dedicado de búsqueda y consulta (o un *frontend* optimizado) para el acceso a documentos históricos y de valor permanente.

- Este portal debe estar diseñado para el perfil de investigadores, entes de control, auditorías internas y la ciudadanía en general, permitiendo búsquedas avanzadas por metadatos descriptivos (PREMIS), fechas y palabras clave (*Full-Text Search*).

- El portal debe garantizar la facilidad de uso (*Usability*) para asegurar que el patrimonio sea realmente accesible.

Filtro de Seguridad Riguroso (Ley 1712 y Ley 1581):

- Control Crítico: Todo acceso y visualización de documentos a través de este portal debe pasar por un filtro de seguridad riguroso y en tiempo real que aplique las restricciones de acceso a la información pública (Ley 1712) y la protección de datos personales (Ley 1581).

- El sistema debe identificar si el documento (o parte de él) sigue bajo reserva legal. Si un documento contiene datos personales sensibles, pero es de interés público, el SGDEA debe facilitar herramientas para la redacción digital (*redaction*) controlada antes de su publicación o visualización, protegiendo la confidencialidad.

Generación de Copias Auténticas y *Self-Service*:

- El sistema debe permitir a los usuarios autorizados o al público generar y descargar copias auténticas y verificables de los documentos públicos y desclasificados.

- Estas copias deben incorporar mecanismos de verificación de autenticidad (ej. códigos QR o *watermarks* con URL de verificación) que permitan al receptor validar que la copia descargada corresponde exactamente al original custodiado en el SGDEA.

- Para entes de control, el sistema debe facilitar el acceso seguro y la descarga masiva de expedientes conforme a los requerimientos de la auditoría.

8.7. Monitoreo, reporte y auditoría del cumplimiento

Esta funcionalidad es la traducción de la Pista de Auditoría Forense (Capítulo 6.4) en indicadores de gestión y de cumplimiento. Asegura que los líderes archivísticos, los gerentes de proceso y los entes de control tengan las herramientas necesarias para medir el desempeño operativo y validar el cumplimiento normativo del SGDEA de manera continua.

Motor de Reportes y KPIs (Indicadores Clave de Desempeño):

- El SGDEA debe contar con un Motor de Reportes que permita generar informes predefinidos y personalizados sobre el estado del sistema.

- Se exige un *Dashboard* de Monitoreo en Tiempo Real que muestre los Indicadores Clave de Desempeño (KPIs) críticos, tales como: Tiempo promedio de respuesta a trámites (conectado al Motor de Plazos), Tasa de cumplimiento de TRD (aplicación del Motor de Retención), Volumen de radicación por dependencia y Densidad de incidentes de seguridad/acceso denegado.

Auditoría de Cumplimiento Normativo:

- La plataforma debe permitir la generación de reportes de auditoría enfocados en el cumplimiento archivístico, demostrando que la documentación ha seguido las reglas de clasificación (CCD) y retención (TRD) sin desviaciones.

- Debe facilitar la exportación forense controlada de los registros de auditoría (logs) para su análisis externo por parte de entes de control (ej. Contraloría, Procuraduría), asegurando la inmutabilidad de los datos exportados.

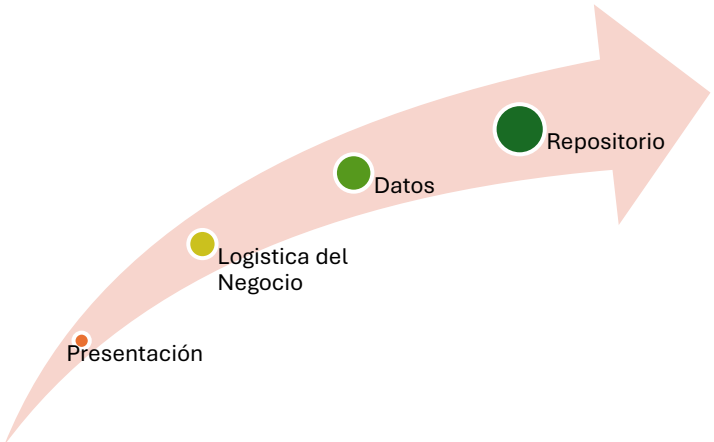
Monitoreo de la Salud Operacional:

- Monitoreo continuo de la salud de los componentes clave: estado del Motor de Retención, disponibilidad de las APIs de Interoperabilidad y el estado de la Verificación Periódica de Integridad de los repositorios de preservación (Capítulo 8.5). Esto es fundamental para la detección proactiva de fallas.

9. Diseño preliminar de arquitectura tecnológica

El diseño de la arquitectura tecnológica es el cimiento ineludible y estratégico sobre el cual se construirá la seguridad, el rendimiento y la sostenibilidad a largo plazo del SGDEA. Dado el carácter crítico y probatorio del sistema para la Alcaldía—al ser el custodio de la memoria institucional y de la fe pública—, este diseño debe garantizar la confiabilidad inquebrantable, la alta disponibilidad y la preservación inmutable del acervo documental. La arquitectura debe estar intrínsecamente blindada, en estricta alineación con los estándares internacionales de seguridad (ISO/IEC 27001) y el modelo de referencia archivístico (OAIS - ISO 14721).

Diagrama de Arquitectura Lógica del SGDEA:



El diseño preliminar no se limita a la selección de servidores, sino que se estructura en cuatro ejes estratégicos que definen la viabilidad técnica y financiera del proyecto:

- Modelo de Despliegue: El modelo de despliegue es una decisión de arquitectura estratégica que balancea el Costo Total de Propiedad (TCO), el rendimiento y los requisitos legales de seguridad y soberanía de datos. La evaluación debe ser rigurosa para seleccionar la opción óptima entre las modalidades *on-premise*, nube pública/privada o híbrida.

    - Análisis de la Soberanía de Datos y Cumplimiento Legal. Antes de cualquier selección, se debe realizar un análisis exhaustivo para garantizar que la solución cumpla con los requisitos de soberanía de datos colombianos para entidades públicas. Esto es crítico si se considera un modelo de nube, donde la ubicación física de los datos primarios y de respaldo debe ser verificable y debe cumplir con la Ley 1581 de 2012 (Protección de Datos) y los requerimientos del AGN.

    - TCO y Elasticidad del Modelo. La decisión debe basarse en el análisis de TCO a 5-7 años (Capítulo 6.1), comparando los costos de capital (CAPEX) de la infraestructura *on-premise* versus los costos operativos (OPEX) de la nube; también el modelo de despliegue debe garantizar la elasticidad. Un modelo basado en la nube (o híbrido con componentes *cloud*) facilita la escalabilidad inmediata para absorber picos de demanda o el crecimiento exponencial de la volumetría sin requerir grandes inversiones iniciales de *hardware*.

    - Definición del Modelo Óptimo (On-premise / Nube Híbrida): Recomendación Estratégica: Se priorizará un Modelo Híbrido o de Nube Privada/Gubernamental, donde los componentes críticos (ej. Archivo Histórico y Repositorios de Preservación Inmutable) residan en entornos de alta seguridad y control (o en la nube bajo esquemas de soberanía controlada). Los componentes de interoperabilidad y *front-end* (ej. Portal VUE, APIs) pueden residir en la nube pública para garantizar la alta disponibilidad y la accesibilidad ciudadana; por otro lado, la arquitectura debe utilizar contenedores o microservicios (ej.

Docker/Kubernetes) para garantizar la portabilidad de la solución entre entornos (on-premise y nube) si es necesario en el futuro.

- Rendimiento y Escalabilidad: son Requerimientos No Funcionales (RNF) críticos que determinan la capacidad del SGDEA para sostener la operación diaria y absorber el crecimiento exponencial de la documentación proyectado para la Alcaldía Mayor de Cartagena. No cumplir con estos RNF convierte la mejor solución funcional en un cuello de botella operacional.

    - Definición Rigurosa de Requerimientos No Funcionales (RNF): Volumetría Proyectada: El diseño debe basarse en un análisis formal de la tasa de crecimiento documental (ej. 15-20% anual) y la proyección de volumen total de almacenamiento (ej. a 5 y 10 años), asegurando que la arquitectura de *storage* sea dimensionada correctamente; Latencia Crítica: Se deben establecer umbrales máximos de latencia para las operaciones críticas, tales como radicación/Ingreso que sea menos de un segundo; consulta por metadatos que sea menos de 2 segundos; Consulta de Contenido (*Full-Text Search*), menos de 5 segundos, incluso con millones de documentos; ejecución de *Workflows*, asignación y transferencia de tareas.

    - Estrategia de Escalabilidad (*Scaling*): Escalabilidad Horizontal (*Horizontal Scaling*): La arquitectura debe ser modular y distribuida (basada idealmente en microservicios o contenedores - Capítulo 9.1) para permitir la adición de nuevos nodos de procesamiento (servidores) y bases de datos sin reconfigurar toda la solución. También se trabaja en la separación de Componentes: El diseño debe separar claramente los componentes que requieren alta velocidad (ej. la base de datos de metadatos transaccionales y el motor de búsqueda) de aquellos que requieren alta capacidad (ej. el repositorio de preservación WORM), permitiendo escalar cada capa de forma independiente.

    - Optimización de Consulta y Búsqueda Masiva: El Motor de Búsqueda debe estar diseñado para soportar consultas masivas y simultáneas (ej. consultas de *Full-Text Search* en archivos indexados) sin degradar el

rendimiento de las operaciones transaccionales (radicación/firma). Esto a menudo requiere la implementación de tecnologías de indexación especializada y la optimización de las consultas para aprovechar al máximo los metadatos de clasificación (CCD/TRD) como filtros primarios.

- Capacidad Transaccional Máxima: El sistema debe ser sometido a pruebas de estrés (Stress Testing) para validar su capacidad máxima de transacciones (ej. documentos radicados por hora, usuarios concurrentes en *worklfows*), garantizando que pueda manejar los picos de demanda generados, por ejemplo, en los cierres contables o los períodos de licitación.

- Sostenibilidad y Soporte (Gobernanza Técnica): La sostenibilidad técnica y el modelo de soporte son pilares que aseguran la longevidad del SGDEA y evitan el riesgo de obsolescencia funcional y tecnológica a mediano y largo plazo. La Gobernanza Técnica establece los mecanismos de control para mantener el sistema actualizado, seguro y funcional de forma continua.

  - Modelo de Soporte Especializado y Niveles de Servicio (SLA): Se debe establecer un Modelo de Soporte Técnico Especializado con una clara definición de los Niveles de Servicio (SLA). Esto incluye la definición de tiempos máximos de respuesta (*Time-to-Respond*) y de solución (*Time-to-Resolve*) para incidentes críticos (ej. fallas en la radicación, indisponibilidad del Motor de Retención). La estructura de soporte debe ser escalonada (Nivel 1 - Soporte de Usuario, Nivel 2 - Soporte Funcional y Archivístico, Nivel 3 - Soporte Técnico Especializado del Proveedor/TI).

  - Mantenimiento Evolutivo y Vigilancia Tecnológica Continua: El mantenimiento no puede ser meramente correctivo. Se exige un plan de Mantenimiento Evolutivo que garantice que la plataforma se adapte a los cambios en el ecosistema legal y tecnológico. Por otro lado, con la Vigilancia Tecnológica: Este plan debe incluir la Vigilancia Tecnológica Continua de la plataforma, monitoreando la obsolescencia de los componentes de *software* (bases de datos, *frameworks*, librerías) y las nuevas amenazas de seguridad (alineado con la ISO/IEC

27001). Por último, El sistema debe implementar un ciclo de actualizaciones de seguridad y parches programado y obligatorio para mitigar proactivamente las vulnerabilidades.

- Transferencia de Conocimiento y Autonomía Interna: Un requisito de sostenibilidad es la Transferencia de Conocimiento formal y exhaustiva al equipo de TI y al equipo Archivístico de la Alcaldía. El objetivo es lograr la autonomía interna para la gestión de la plataforma (ej. parametrización autónoma de TRD, *Workflows*, roles RBAC), reduciendo la dependencia a largo plazo de consultores o proveedores externos y optimizando el TCO (Capítulo 6.1 y 6.5).

- Gestión de Licencias y Dependencias: El modelo de soporte debe incluir una gestión centralizada y proactiva de licencias de *software* propietario y de las dependencias de *software* libre utilizadas, asegurando la renovación oportuna y la conformidad con los términos de uso, previniendo interrupciones operativas por incumplimiento de licencias.

- Resiliencia Operativa (Continuidad del Negocio): La Resiliencia Operativa es un requisito no funcional de máxima criticidad para el SGDEA, el cual debe garantizar la operatividad continua y la protección irrefutable de los documentos, incluso en el escenario de fallas catastróficas. Este diseño asegura la capacidad de la Alcaldía para responder a cualquier contingencia tecnológica.

  - Alta Disponibilidad (HA) y Tolerancia a Fallos: El diseño de la arquitectura debe ser tolerante a fallos (*Fault-Tolerant*) mediante la implementación de Alta Disponibilidad (HA). Esto implica la duplicación de los componentes críticos (servidores de aplicación, bases de datos y repositorios) en una configuración activa/activa o activa/pasiva. También la conmutación por error (*Failover*) entre los componentes debe ser automática y transparente para el usuario final, asegurando que la indisponibilidad del servicio por fallos de *hardware* o *software* sea mínima.

- Plan de Recuperación ante Desastres (DRP) Formal: Se exige la creación de un Plan de Recuperación ante Desastres (DRP) explícito para el SGDEA, con la implementación de un Sitio Alterno de Recuperación (DR Site), preferiblemente en una ubicación geográficamente separada (alineación con la Resiliencia Geográfica del Capítulo 8.5). Por otro lado, el DRP debe definir formalmente el RTO (*Recovery Time Objective*)—el tiempo máximo que el sistema puede estar inactivo—y el RPO (*Recovery Point Objective*)—la cantidad máxima de datos que se permite perder—. Ambas métricas deben ser estrictas y ajustarse a la criticidad probatoria del sistema.

- Respaldo Continuo y Estrategia de Retención: Se debe implementar una estrategia de Respaldo Continuo (o replicación) de los datos (metadatos y binarios) con un esquema de retención que incluya copias diarias, semanales y mensuales, almacenadas tanto en el sitio principal como en el sitio alterno. También el sistema debe implementar pruebas periódicas de restauración de los respaldos para validar la integridad de los datos y la efectividad del DRP, asegurando que los datos puedan ser recuperados tal como se necesita en caso de una contingencia real.

- Monitoreo de Continuidad: La arquitectura debe incluir herramientas de monitoreo 24/7 para vigilar el estado de los componentes de HA y DR, generando alertas inmediatas ante la degradación del rendimiento o la falla de los sistemas de replicación.

9.1 Evaluación del modelo de despliegue: nube vs. local vs. híbrido

La elección del modelo de despliegue constituye la decisión arquitectónica fundacional del SGDEA, impactando directamente su Costo Total de Propiedad (TCO), su resiliencia operativa, la flexibilidad de escalabilidad y su marco de seguridad. Esta selección no es meramente técnica, sino altamente estratégica y está supeditada a un análisis financiero riguroso que evalúe los costos iniciales (CAPEX) frente a los costos operativos (OPEX) a largo plazo. De manera crítica, la decisión final debe garantizar el cumplimiento ineludible con la normativa colombiana, especialmente en lo relativo a la soberanía y protección de datos

(Ley 1581 de 2012), asegurando que la ubicación y el control del Archivo Histórico se mantengan bajo la autoridad legal de la Alcaldía. El modelo seleccionado (sea *on-premise*, nube o híbrido) debe ser el que mejor equilibre la demanda de rendimiento con la garantía de cumplimiento legal y la máxima disponibilidad.

9.1.1. Infraestructura Local (On-Premise)

La infraestructura local, u *on-premise*, representa el modelo tradicional en el que la Alcaldía mantiene el control físico y lógico absoluto sobre la totalidad de la pila tecnológica que soporta el SGDEA. En este esquema, la entidad asume la responsabilidad y los costos de adquirir, instalar y gestionar todos los componentes, desde el *hardware* (servidores, almacenamiento, redes) hasta el *software* base y los sistemas de seguridad, residiendo todo dentro de su propio centro de datos o en uno contratado bajo su control directo.

Ventajas Estratégicas (Control y Cumplimiento Normativo):

- Soberanía y Control Físico Total: Otorga el máximo nivel de control sobre la seguridad física, la configuración de red y la soberanía de los datos. Esto es crucial para los documentos con la más alta clasificación de reserva o seguridad nacional, ya que la ubicación de los datos es garantizada y facilita las auditorías *in-situ* de los entes de control.

- Cumplimiento Normativo Simplificado: Puede ser la opción más directa y sencilla para demostrar el cumplimiento estricto de las normativas colombianas que imponen restricciones sobre la localización geográfica de datos para información clasificada o reservada, eliminando las complejidades contractuales y legales asociadas a la nube.

- Rendimiento en Redes Internas: Para la operación interna y los usuarios ubicados en el mismo centro de datos, puede ofrecer una latencia mínima

y un rendimiento muy alto, especialmente para el acceso a documentos voluminosos.

Desafíos Críticos (Costo y Gestión):

- Alta Inversión Inicial (CAPEX): Exige una inversión de capital (CAPEX) sustancialmente alta y concentrada para la adquisición de *hardware* de alta disponibilidad (HA), licencias de *software* base, la adecuación física del centro de datos (climatización, seguridad contra incendios) y los sistemas de respaldo eléctrico.

- Costos Operativos (OPEX) Elevados y Riesgo de Obsolescencia: Los costos operativos (OPEX) son significativos, ya que la Alcaldía es responsable del mantenimiento, el consumo energético, el monitoreo 24/7 y la gestión de la obsolescencia. Esto exige la contratación o especialización de personal técnico altamente calificado para la administración continua de toda la pila tecnológica.

- Escalabilidad Rígida y Lenta: El escalamiento del sistema (Capítulo 9.2) es inherentemente más lento, rígido y costoso, ya que está limitado por la capacidad del *datacenter* y requiere procesos de planeación, adquisición y configuración de nuevo *hardware* ante cada necesidad de crecimiento.

- Resiliencia Operativa Limitada: La implementación de la Alta Disponibilidad (HA) y la Recuperación ante Desastres (DRP) es más costosa, ya que exige la duplicación de la infraestructura en un sitio alterno geográficamente distante gestionado por la propia entidad.

En conclusión, la Infraestructura Local es la opción que ofrece el máximo control sobre el activo documental y la mayor simplicidad para demostrar el cumplimiento de la soberanía de datos. Sin embargo, es el modelo con el mayor

riesgo de ineficiencia de costos (alto TCO) debido a la alta inversión inicial y los costos operativos fijos por administración y obsolescencia. Se considera ideal solo para la capa de preservación y seguridad máxima, donde los requisitos de inmutabilidad y soberanía priman sobre la necesidad de elasticidad y *scaling* rápido. No obstante, no es la opción más flexible para el entorno transaccional del SGDEA.

9.1.2 Infraestructura en la nube (Cloud Computing - IaaS/PaaS)

La Infraestructura en la Nube (sea pública, privada o comunitaria) representa un cambio paradigmático en la adquisición de recursos tecnológicos. En este modelo, la Alcaldía contrata y accede a los recursos de cómputo, almacenamiento, bases de datos y red a través de un proveedor de servicios (*Cloud Service Provider* - CSP). El modelo de consumo puede ser IaaS (Infraestructura como Servicio), donde la Alcaldía gestiona el sistema operativo y el *software*, o PaaS (Plataforma como Servicio), donde el proveedor gestiona la mayor parte de la pila, permitiendo a la Alcaldía enfocarse solo en la aplicación SGDEA.

Ventajas Estratégicas (Elasticidad y Resiliencia Financiera):

- Flexibilidad, Elasticidad y Escalabilidad Inmediata: Provee una capacidad de escalamiento prácticamente ilimitada. El sistema puede aumentar o reducir dinámicamente recursos (CPU, RAM, almacenamiento) de forma elástica, permitiendo responder a picos de demanda o al crecimiento exponencial de la volumetría proyectada sin la necesidad de adquirir *hardware* de forma anticipada y sobredimensionada (Capítulo 9.2).

- Optimización Financiera y Reducción de CAPEX: Se elimina o reduce drásticamente la inversión de capital (CAPEX) inicial en *hardware* e infraestructura de centro de datos. El modelo se convierte en un gasto operativo (OPEX) que se ajusta al uso real (*pay-as-you-go*), lo que mejora la gestión presupuestaria y la liquidez de la Alcaldía.

- Alta Disponibilidad (HA) y Resiliencia Gestionada: Los proveedores de nube ofrecen por defecto servicios gestionados de alta disponibilidad (HA), replicación geográfica y respaldo automatizado. Esto simplifica significativamente la implementación de los exigentes Planes de Recuperación ante Desastres (DRP) y la obtención de los RTO/RPO requeridos (Capítulo 9.4).

Desafíos Críticos (Soberanía y Dependencia):

- Soberanía y Localización de Datos (Riesgo Crítico): Es el desafío más importante. Es crucial y mandatorio garantizar contractualmente que el proveedor de nube cumpla plenamente con la Ley 1581 de 2012 y que los datos, especialmente la información clasificada, reservada o histórica, residan exclusivamente en Centros de Datos (AZs) ubicados en territorios que ofrezcan un nivel adecuado de protección y preferiblemente, en jurisdicción colombiana. La Alcaldía debe retener el control sobre las claves de cifrado de los documentos sensibles.

- Dependencia y Riesgo de Bloqueo Tecnológico (*Vendor Lock-in*): Existe una dependencia del proveedor para la disponibilidad de la infraestructura y la gestión de la seguridad en las capas inferiores. La migración futura del SGDEA a otro proveedor o a un modelo *on-premise* puede ser compleja y costosa (riesgo de *vendor lock-in*). Esto requiere una gestión de contratos y niveles de servicio (SLAs) extremadamente rigurosa que abarque las cláusulas de salida y portabilidad de datos.

- Seguridad Compartida y Responsabilidad: Bajo el Modelo de Responsabilidad Compartida de la nube, el proveedor asegura la infraestructura base, pero la Alcaldía es la única responsable de la seguridad de la aplicación SGDEA, de los datos, de la configuración de red virtual y de la gestión de identidades y accesos (RBAC).

En conclusión, la Nube es el modelo que ofrece la mayor agilidad, la mejor respuesta al crecimiento exponencial (escalabilidad) y la mayor facilidad para implementar la resiliencia operativa y el DRP a bajo costo. Es el modelo ideal para los componentes que requieren alta elasticidad (ej. el Portal VUE, APIs de Interoperabilidad). Sin embargo, su viabilidad para el SGDEA está directamente condicionada y supeditada a la capacidad de la Alcaldía de obtener garantías contractuales y técnicas irrefutables de que la soberanía y la protección de los datos cumplen al 100% con la legislación colombiana.

9.1.3 Modelo Híbrido

El Modelo Híbrido se presenta como la estrategia arquitectónica óptima y de menor riesgo para el SGDEA de la Alcaldía. Combina inteligentemente las fortalezas de la infraestructura local (on-premise) con la elasticidad y la eficiencia de la nube (cloud computing), permitiendo una gestión de riesgos por capas y la optimización del TCO. La clave de este modelo radica en ubicar cada componente del SGDEA en el entorno que mejor se ajuste a su criticidad, su volumen y sus requisitos legales.

Casos de Uso Estratégicos (Riesgo y Eficiencia):

- Almacenamiento por Niveles y Soberanía de Datos: Capa Crítica (Local/Nube Privada): Mantener los documentos activos, transaccionales y la información más sensible o clasificada (*Clasificada/Reservada*) *on-premise* o en una Nube Gubernamental/Privada con control de soberanía irrefutable. También se tiene la capa de Preservación y Respaldo (Nube de Bajo Costo): Utilizar servicios de almacenamiento en la nube de bajo costo y alta durabilidad (ej. *Cold Storage* o almacenamiento de archivo) para copias de respaldo de largo plazo y para el Archivo Histórico de baja consulta (Capítulo 8.5), optimizando el TCO al pagar tarifas mínimas de almacenamiento.

- Contingencia y DRP (*Disaster Recovery as a Service*): Utilizar la nube como el Sitio de Recuperación ante Desastres (DRaaS). El *backup* y la réplica del sistema transaccional se mantienen listos en la nube, permitiendo una conmutación por error (*Failover*) rápida y eficiente en caso de una falla catastrófica en el centro de datos principal de la Alcaldía. Esto garantiza los RTO y RPO (Capítulo 9.4) de manera rentable.

- Desarrollo, Pruebas y *Business Agility*: Desplegar los entornos de Desarrollo, Pruebas y Aseguramiento de Calidad (QA) en la nube. Esto permite a los equipos de TI y a los proveedores utilizar recursos bajo demanda para agilizar los ciclos de implementación, pruebas de estrés y despliegue de nuevas funcionalidades sin afectar o impactar los recursos del entorno de Producción (*on-premise*).

- Servicios de Alto Tráfico (*Front-End*): Alojar el Portal VUE (Ventanilla Única Electrónica) y las APIs de Interoperabilidad (Capítulo 8.2) en la nube pública. Esto garantiza la elasticidad necesaria para soportar altos volúmenes de tráfico ciudadano o de sistemas externos, asegurando la accesibilidad y el rendimiento público.

En conclusión, un Modelo Híbrido permite a la Alcaldía mitigar los principales desafíos de los modelos puros: el alto costo de escalabilidad de *On-Premise* se resuelve con la nube, y el riesgo de soberanía de la nube se resuelve manteniendo los datos más críticos localmente. Este modelo proporciona la flexibilidad, el control, el cumplimiento legal y la eficiencia de costos que requiere un proyecto de la envergadura del SGDEA.

9.2 Requerimientos mínimos de escalabilidad y desempeño

El rendimiento y la escalabilidad son Requerimientos No Funcionales (RNF) de la más alta prioridad, esenciales para garantizar que el SGDEA conserve una experiencia de usuario fluida y eficiente a pesar del alto volumen de

transacciones diarias, las consultas masivas y el crecimiento exponencial de la volumetría documental (Capítulo 9).

- Escalabilidad Horizontal (*Horizontal Scaling*) como Principio Arquitectónico: La arquitectura de la aplicación debe estar diseñada bajo el principio de escalabilidad horizontal. Esto significa que, en lugar de depender de servidores monolíticos más potentes (escalamiento vertical, costoso y limitado), la capacidad del sistema se aumentará mediante la adición de nuevos nodos de aplicación detrás de un Balanceador de Carga (Load Balancer). Esto asegura la distribución equitativa del tráfico y la carga de trabajo entre los recursos disponibles, optimizando la inversión y asegurando la disponibilidad.

- Arquitectura Desacoplada y Orientada a Microservicios: Se exige una arquitectura por capas desacoplada o un diseño de microservicios, donde cada componente principal pueda operar y escalar de forma independiente: *Frontend*, lógica de negocio (*Backend*), Base de Datos Transaccional, Motor de Búsqueda y Repositorio de Archivos Binarios. También el SGDEA debe utilizar un motor de búsqueda de texto completo dedicado (ej. *Elasticsearch* o similar), separado de la base de datos transaccional, para soportar la indexación rápida y las consultas masivas sin degradar el rendimiento de la radicación y los *workflows*.

- Métricas de Desempeño (KPIs): Se definirán y medirán indicadores clave de rendimiento, tales como:
    - Tiempo de respuesta para operaciones clave: Búsqueda (< 3 segundos), radicación de un documento (< 5 segundos), visualización de un documento (< 2 segundos).
    - Disponibilidad del servicio: Objetivo de > 99.5% en horario laboral.
    - Usuarios Concurrentes: Soportar el número de usuarios concurrentes proyectado en la fase de diagnóstico con una degradación mínima del rendimiento.

- Monitoreo y Alertas Proactivas: Implementar herramientas de monitoreo (APM - Application Performance Monitoring) que vigilen el consumo de CPU, memoria, I/O de disco y tráfico de red, y que generen alertas automáticas cuando se superen umbrales predefinidos, permitiendo al equipo de TI actuar antes de que ocurra una falla.

    - Monitoreo de Rendimiento de Aplicación (APM): Implementar herramientas de APM que vigilen continuamente el rendimiento de la aplicación, el consumo de CPU, memoria, I/O de disco y tráfico de red.

    - Alertas Proactivas: El sistema debe generar alertas automáticas e inmediatas al equipo de TI cuando el consumo supere los umbrales predefinidos (ej. CPU > 80% durante 15 minutos), permitiendo la intervención proactiva (ej. escalar recursos) antes de que el rendimiento se vea afectado u ocurra una falla.

9.2.1 Modelo de datos y tecnología de base (BD)

La selección y el diseño del Modelo de Datos son determinantes para el rendimiento y la integridad transaccional del SGDEA.

- Motor Dual (Relacional + Documental): Se priorizará el uso de un Motor de Base de Datos relacional con capacidad de manejar datos JSONB (ej. PostgreSQL) o una tecnología similar.

    - Relacional (SQL): Para garantizar la integridad transaccional (ACID) y la robustez de los metadatos críticos (fechas, CCD, TRD, *workflows*).

    - Documental (NoSQL/JSONB): Para gestionar la flexibilidad y la indexación rápida de metadatos complejos y variados de preservación (PREMIS) o para el *logging* de la Pista de Auditoría, sin sacrificar la integridad transaccional.

- Optimización para Lectura y Escritura: El diseño de la BD debe ser optimizado para manejar un alto volumen de escrituras (radicación) y lecturas (consultas) de forma simultánea, en cumplimiento con las métricas de latencia (Capítulo 9.2).
- Separación Lógica: Se mantendrá una separación lógica entre la Base de Datos Transaccional (OLTP) y el repositorio de búsqueda de texto completo (Motor Dedicado), para garantizar que las consultas masivas no afecten el rendimiento de las operaciones diarias.

9.3 Modelo de sostenibilidad y soporte post-implementación

La puesta en marcha del SGDEA representa el inicio formal de la gestión documental electrónica, no la conclusión del proyecto tecnológico. Para garantizar la continuidad del servicio crítico, la inversión realizada y la longevidad del Archivo Histórico, es imperativo establecer un Modelo de Sostenibilidad y Soporte Post-Implementación rigurosamente estructurado. Este modelo debe asegurar la operación continua 24/7, el mantenimiento evolutivo para adaptarse a los cambios normativos y tecnológicos, y una vigilancia tecnológica proactiva. Una gobernanza técnica eficaz, con roles y responsabilidades claras, es la única garantía de que el SGDEA conservará su valor probatorio y su eficiencia operativa a lo largo de las décadas.

9.3.1. Acuerdos de nivel de servicio (SLA):

La definición de los Acuerdos de Nivel de Servicio (SLA) es una obligación contractual y operacional que formaliza el compromiso del equipo de TI interno o del proveedor externo con la Alcaldía. Los SLAs son el mecanismo de control que asegura que la Resiliencia Operativa se mantenga en la práctica, minimizando el impacto financiero, legal y administrativo de cualquier interrupción.

Disponibilidad del Servicio (*Uptime*) y Criticidad por Módulo:

- Se establecerá un porcentaje mínimo de tiempo que el sistema debe estar en línea. El SGDEA, como sistema crítico, debe aspirar a un 99.9% de

disponibilidad (Tier III) para sus módulos transaccionales (Radicación, *Workflows*, APIs de Interoperabilidad) en horario laboral.

- La disponibilidad puede ser diferenciada: el Portal VUE (acceso ciudadano) y el Motor de Radicación se clasificarán como Críticos (Tier 1), mientras que el acceso al Archivo Histórico puede tener un SLA ligeramente inferior, aunque siempre superior al 99%.

- El cálculo del *uptime* debe excluir las ventanas de mantenimiento programadas.

Tiempos de Respuesta a Incidentes (Escalabilidad de Severidad):

- Se deben definir tiempos máximos rigurosos para acusar recibo, realizar el diagnóstico inicial y comenzar a trabajar en un incidente, categorizados por su severidad e impacto en el negocio:

    - Severidad 1 (Crítico/Bloqueante): Falla total del Motor de Radicación o del Motor de Firma Digital. Tiempo de Respuesta Máximo: 15 minutos (24/7), con escalamiento inmediato al Nivel 3.

    - Severidad 2 (Alto Impacto): Degradación significativa del rendimiento (incumplimiento de RNF del Capítulo 9.2) o falla de un *workflow* esencial. Tiempo de Respuesta Máximo: 1 hora.

    - Severidad 3 (Medio/Menor Impacto): Fallas menores no bloqueantes o errores funcionales no críticos. Tiempo de Respuesta Máximo: 4 a 8 horas.

Tiempos de Resolución (*Time-to-Resolve*) y Análisis de Causa Raíz (RCA):

- Se establecerán Tiempos Objetivo de Resolución para cada nivel de severidad. Para incidentes Críticos (Severidad 1), el tiempo de resolución objetivo debe ser inferior a 4 horas (RTO - Capítulo 9.4).

- Para incidentes recurrentes o de Severidad 1/2, es obligatorio que el proveedor o el equipo de TI entregue un Análisis de Causa Raíz (RCA) en un plazo no mayor a 5 días hábiles después de la resolución, para implementar medidas de prevención y mejora continua.

Ventanas de Mantenimiento y Gestión de Cambios (Change Management):

- Se definirán Ventanas de Mantenimiento estrictamente limitadas a horarios no operacionales (generalmente nocturnos o de fin de semana).

- Cualquier cambio que pueda impactar la disponibilidad debe estar sujeto a un riguroso Protocolo de Gestión de Cambios (Change Management), que incluya la justificación, la evaluación de riesgos, la aprobación por el Comité de TI/Archivístico y la comunicación proactiva a los usuarios con un mínimo de 72 horas de antelación.

Penalidades e Incentivos (Gobernanza Contractual):

- El contrato de soporte debe incluir cláusulas de Penalidades Financieras claras y proporcionales por el incumplimiento reiterado o sustancial de los SLAs de Disponibilidad y Tiempo de Resolución Crítico. Esto es vital para proteger la inversión.

- Se pueden contemplar Incentivos por superar consistentemente los objetivos de desempeño, promoviendo la calidad proactiva del servicio.

9.3.2. Estructura de soporte por niveles:

Para garantizar el cumplimiento de los estrictos Acuerdos de Nivel de Servicio (SLA) (Capítulo 9.3.1), el modelo de soporte debe ser una estructura jerárquica y altamente organizada, con responsabilidades claras y un protocolo de

escalación definido. Esta estructura de tres niveles garantiza que los incidentes se filtren, se prioricen y se resuelvan en el nivel de experiencia más adecuado.

Nivel 1 (Mesa de Ayuda / *Help Desk*): El Filtro Operacional

- Descripción del Rol: Es la primera línea de contacto (Front-Line Filter), manejada por personal interno de la Alcaldía o un proveedor dedicado. Su función principal es la gestión de la comunicación, el diagnóstico inicial y la resolución de incidentes de baja complejidad y alta frecuencia.

- Funciones Clave:
    - Registro y Categorización: Registrar todos los incidentes y solicitudes, asignando la Severidad (Crítico, Alto, Medio) y el Impacto (Número de usuarios afectados) conforme al SLA.
    - Resolución Básica: Resolver consultas funcionales básicas, problemas de acceso (ej. reseteo de contraseña), y validar la conexión de los usuarios.
    - Escalación Controlada: Transferir los incidentes no resueltos al Nivel 2, asegurando que se anexe la información de diagnóstico completa.

- Conocimiento Requerido: Conocimiento funcional básico del SGDEA, excelente servicio al cliente, manejo de la herramienta de gestión de *tickets* y consulta de la Base de Conocimiento (Knowledge Base).

Nivel 2 (Soporte Funcional, Archivístico y Técnico de Aplicación): El Especialista

- Descripción del Rol: Equipo con conocimiento profundo y avanzado del SGDEA. Este nivel se subdivide en funcional/archivístico y técnico, y es

responsable de resolver la mayoría de los incidentes que requieren acceso a la configuración del sistema.

- Funciones Clave:
    - Soporte Archivístico/Funcional: Resolver problemas relacionados con la aplicación del CCD/TRD, errores en la configuración de flujos de trabajo (*Workflows*) (Capítulo 7.1.2) o fallos en la aplicación de los Metadatos Obligatorios.
    - Soporte Técnico de Aplicación: Diagnosticar y resolver errores de bases de datos de bajo nivel, fallos de integración con APIs externas (Capítulo 8.2) y problemas de rendimiento de la aplicación (RNF del Capítulo 9.2).
    - Gestión de Cambios Menores: Ejecutar cambios menores de configuración, previa aprobación del Comité de Cambios.
- Conocimiento Requerido: Experiencia en archivística y gestión documental electrónica, manejo avanzado de SQL para consultas de bases de datos, y comprensión de la arquitectura de la aplicación.

Nivel 3 (Soporte Especializado y Corrección de Código): El Arquitecto

- **Descripción del Rol:** Es el nivel de expertos en el código fuente, la arquitectura y la seguridad. Este soporte es proporcionado por el equipo de desarrollo del producto (si es comercial) o los arquitectos *senior* de la solución (si es a medida). Es el destino final para la resolución de la Severidad 1 (Crítica).

- **Funciones** Clave:
    - Corrección de *Bugs* de Código: Identificar y corregir errores en el código fuente (bugs) que requieran una nueva versión o parche de *software*.
    - Análisis de Causa Raíz (RCA): Realizar el Análisis de Causa Raíz (RCA) formal para incidentes mayores (SLA Capítulo 9.3.1) y proponer soluciones permanentes.
    - Infraestructura Crítica: Resolver problemas complejos de infraestructura relacionados con la Alta Disponibilidad (HA), la replicación de datos, la restauración del DRP (Capítulo 9.4) y los fallos de los motores de preservación (PDF/A).
- Conocimiento Requerido: Arquitectura de *software* (Microservicios/Contenedores), desarrollo de *software* (lenguaje de programación del SGDEA), administración avanzada de bases de datos y experiencia en seguridad (cifrado, DRP/BCP).

9.3.3. Gestión de Cambios y Actualizaciones:

La Gestión de Cambios y Actualizaciones es un proceso de Gobernanza Técnica (alineado con ISO/IEC 27001) que minimiza el riesgo de interrupción operativa, corrupción de datos o introducción de vulnerabilidades de seguridad en el SGDEA. Ninguna modificación, por mínima que sea, puede implementarse sin seguir este protocolo riguroso

Protocolo Formal de Gestión de Cambios (GDC) y Gobernanza:

- Se implementará un Proceso Formal de Gestión de Cambios (GDC) que debe ser gobernado por un Comité de Cambios (*Change Advisory Board* - CAB)

compuesto por representantes de TI, la Dirección de Archivo, y el Oficial de Seguridad.

- Toda modificación (parche de seguridad, nueva funcionalidad, ajuste de *workflow*) debe documentarse mediante una Solicitud de Cambio (RFC) que detalle el alcance, el riesgo potencial, la planificación de *testing* y el plan de *rollback*, antes de obtener la aprobación formal del CAB.

Uso Obligatorio de Múltiples Ambientes:

- Es mandatorio el uso de, al menos, tres entornos segregados y controlados: Desarrollo (DEV), Pruebas/Pre-producción (QA/Staging) y Producción (PROD).

- Toda modificación debe ser probada rigurosamente en el entorno de QA/Staging, utilizando datos anónimos o enmascarados y simulando las condiciones de carga de trabajo real, para validar su estabilidad, rendimiento y el cumplimiento de los RNF (Capítulo 9.2).

Calendario de Actualizaciones y Aplicación Expedita de Parches Críticos:

- Se mantendrá un Calendario de Actualizaciones Funcionales (Mantenimiento Evolutivo) planificado con antelación, que debe ejecutarse dentro de las Ventanas de Mantenimiento definidas en el SLA (Capítulo 9.3.1).

- Parches de Seguridad Críticos: Los parches que corrijan vulnerabilidades de seguridad crítica deben ser priorizados y aplicados de manera expedita, con un tiempo máximo de resolución e implementación no mayor a 72 horas desde su liberación oficial, incluso si requieren una ventana de mantenimiento

de emergencia. La seguridad y la integridad del sistema priman sobre el calendario funcional.

Pruebas de Regresión y Plan de *Rollback* (Retorno):

- Toda actualización debe incluir pruebas de regresión para confirmar que las funcionalidades existentes y críticas (ej. Radicación, Firma Digital) no han sido afectadas por el cambio.

- Se exige un Plan de *Rollback* (Retorno) detallado y validado, asegurando que, si la implementación en Producción falla o introduce un error grave, el sistema pueda volver a su estado funcional anterior de forma rápida, segura y sin ninguna pérdida de los datos transaccionales, utilizando el último respaldo validado.

9.3.4. Capacitación Continua y Gestión del Conocimiento

La capacitación y la gestión del conocimiento son esenciales para asegurar la adopción efectiva y la operación correcta del SGDEA, mitigando el riesgo de errores de usuario que comprometan la integridad documental o el cumplimiento normativo. Este proceso debe ser continuo, no limitado a la fase inicial de implementación.

- Programa Formal de Reentrenamiento y Especialización Anual:

    - Se establecerá un Programa Formal y Obligatorio de Reentrenamiento y Recertificación Anual para todos los perfiles de usuario (archivistas, administradores del sistema y usuarios finales).
    - El reentrenamiento debe enfocarse en: Novedades Funcionales: Cambios introducidos por el mantenimiento evolutivo (Capítulo 9.3.3); Refuerzo Normativo: Énfasis en los principios archivísticos (CCD, TRD,

Disposición Final) y las implicaciones legales del uso del SGDEA; Seguridad: Refuerzo en las mejores prácticas de seguridad, gestión de permisos (RBAC) y la prevención de incidentes de seguridad.

- Se diseñarán Módulos de Capacitación Especializada para roles críticos (ej. Administradores de Archivo, Oficiales de Seguridad, Jefes de Dependencia), enfocados en el uso correcto de las funcionalidades avanzadas.

- Base de Conocimiento Centralizada y Autoayuda (*Self-Service*):

  - Se debe crear y mantener una Base de Conocimiento (Knowledge Base) centralizada e integrada al SGDEA. Este repositorio debe contener material de apoyo de fácil acceso y uso: Manuales Operacionales Detallados para cada módulo; Guías Rápidas y Listas de Verificación (*Checklists*) para tareas críticas (ej. Radicación de un expediente, Firma Digital); Videos Tutoriales Breves y módulos de *e-learning* para la incorporación de nuevos funcionarios.
  - La Base de Conocimiento debe ser un recurso vivo, mantenido y actualizado continuamente (responsabilidad del Nivel 2 de Soporte, Capítulo 9.3.2), para facilitar la autoayuda (*Self-Service*) y reducir la carga de la Mesa de Ayuda (Nivel 1).

- Módulos de Formación Obligatoria para Nuevos Funcionarios:

  - El proceso de *onboarding* (incorporación) de nuevos funcionarios debe incluir la aprobación de un módulo de formación básica sobre el uso del SGDEA y la normativa archivística como requisito previo para la asignación de roles y permisos de acceso (RBAC).

9.4 Continuidad operativa, respaldo y recuperación ante desastres (BCP/DRP)

El SGDEA es un sistema de misión crítica cuya indisponibilidad no solo paraliza la operación administrativa de la Alcaldía, sino que compromete directamente el valor probatorio, la fe pública y la legalidad de los documentos que custodia. Por tanto, la arquitectura de este sistema debe ser intrínsecamente resiliente por diseño, asegurando la protección contra cualquier tipo de falla, ya sea por *hardware*, *software* o desastre natural. Este capítulo detalla el diseño explícito de mecanismos de Alta Disponibilidad (HA) y la estrategia de Respaldo y Recuperación ante Desastres (DRP), en el marco de un Plan de Continuidad del Negocio (BCP) formal. El objetivo final es garantizar una operatividad ininterrumpida y cumplir con métricas estrictas de tiempo y punto de recuperación (RTO y RPO) que protejan la integridad y disponibilidad de la memoria institucional ante cualquier contingencia.

9.4.1. Análisis de impacto al negocio (BIA) y definición de RTO/RPO

La base de todo Plan de Continuidad del Negocio (BCP) y Recuperación ante Desastres (DRP) es el Análisis de Impacto al Negocio (BIA). Este es un proceso formal y obligatorio que identifica las funciones críticas del SGDEA y cuantifica las consecuencias financieras, legales y de reputación de su interrupción. Solo a través del BIA se pueden establecer las métricas de recuperación que guiarán el diseño arquitectónico del sistema.

El BIA debe definir rigurosamente dos métricas temporales obligatorias:

- RTO (*Recovery Time Objective* - Objetivo de Tiempo de Recuperación): Definición: El tiempo máximo aceptable que el sistema, la aplicación o una función crítica pueden permanecer inactivos tras un evento de desastre. El RTO define la velocidad con la que el SGDEA debe volver a la operación; Requisito Crítico: Dado que el Motor de Radicación y el Motor de Firma

Digital son funciones de Fe Pública y Legales, sus RTO deben ser extremadamente bajos (Ejemplo RTO para Radicación: ≤ 4 horas (para la restauración del servicio transaccional; Ejemplo RTO para Consulta (Archivo Histórico): ≤ 8 horas.)

- RPO (*Recovery Point Objective* - Objetivo de Punto de Recuperación): Definición, La cantidad máxima de pérdida de datos que es aceptable, medida en tiempo. El RPO define la frecuencia con la que deben ejecutarse los respaldos o la replicación de datos para cumplir con el umbral de pérdida; Requisito Crítico: El SGDEA no puede permitirse una pérdida de datos significativa sin comprometer su valor probatorio.

    - Ejemplo RPO para Metadatos y Documentos Transaccionales: ≤ 15 minutos. Esto exige una replicación continua o síncrona/asíncrona entre el sitio primario y el sitio de DR, en lugar de un respaldo diario, para proteger los documentos recién radicados o modificados.

    - Ejemplo RPO para Archivo Histórico: ≤ 24 horas (dada su inmutabilidad y baja frecuencia de cambio).

La definición de un RPO bajo es la que impulsa la necesidad de implementar soluciones de replicación de bases de datos y almacenamiento en tiempo real (Capítulo 9.4.3), y no solo soluciones de *backup* tradicional.

9.4.2. Estrategia de respaldos 3-2-1:

La estrategia de respaldos es la última línea de defensa contra la pérdida catastrófica de la información y debe ser diseñada para cumplir con los estrictos RPO (Objetivo de Punto de Recuperación) definidos por el BIA (Capítulo 9.4.1). Se implementará una política de respaldos inviolable y auditable que sigue el estándar de seguridad de datos globalmente reconocido: la Regla 3-2-1.

- **La Regla de respaldo 3-2-1 (el estándar global de protección de datos):**
    - 3 Copias: Se mantendrán siempre un mínimo de tres (3) copias completas del conjunto de datos del SGDEA (la copia productiva activa y dos copias de respaldo). Esto minimiza el riesgo de que dos fallas simultáneas comprometan todos los datos.
    - 2 Soportes Distintos: Las copias de respaldo deben almacenarse en al menos dos (2) tipos de medios diferentes. Esto protege contra fallas específicas de un medio (ej. fallas de disco duro). Los medios pueden incluir una combinación de: *Discos de Alto Rendimiento (SAN/NAS)*, *Cinta Magnética* (para archivo a muy largo plazo) o Dos Servicios de Almacenamiento en la Nube distintos (evitando la dependencia de una única infraestructura).
    - 1 Copia *Off-site* (Fuera de Sitio): Se mantendrá obligatoriamente al menos una (1) copia de respaldo en una ubicación geográfica separada y segura (*off-site*). Esta copia es la garantía contra desastres locales que puedan destruir el centro de datos principal y el sitio de respaldo cercano (ej. incendio, inundación), asegurando la continuidad del negocio (Capítulo 9.4).

- Pruebas de restauración obligatorias y verificación de integridad**:**
    - Los respaldos no son válidos si no son restaurables. Es obligatorio realizar Pruebas de Restauración completas y documentadas al menos trimestralmente, simulando el proceso de recuperación ante desastres en el Sitio Alterno (DR Site).
    - Verificación Forense: Durante estas pruebas, el sistema debe validar la integridad de los datos restaurados mediante el cálculo del Hash Criptográfico (Checksum) del archivo, comparándolo con el *hash* original registrado en los metadatos de preservación (Capítulo 8.3.2). Esto garantiza que el respaldo no haya sufrido corrupción durante el almacenamiento.

- Inmutabilidad de los respaldos (*Immutability*):
    - Los respaldos críticos (especialmente las copias *off-site*) deben almacenarse utilizando políticas de inmutabilidad, lo que significa que no pueden ser modificados o eliminados durante un período de tiempo definido. Esta capa de seguridad adicional protege los datos contra ataques de *ransomware* o eliminaciones maliciosas que busquen comprometer tanto el sistema productivo como sus copias de respaldo.

9.4.3. Diseño para alta disponibilidad (HA):

La Alta Disponibilidad (HA) es la arquitectura diseñada para minimizar el tiempo de inactividad (downtime) de las operaciones críticas del SGDEA, asegurando que un fallo de hardware o software en un componente individual no detenga la operación de la Alcaldía. El diseño de HA se basa en la redundancia activa de todos los componentes de la capa transaccional.

- **Clústeres de base de datos y replicación activo-pasivo/activo-activo:**
    - Las Bases de Datos (BD) transaccionales (que contienen los metadatos críticos de radicación y workflows) deben configurarse en un esquema de Clúster de Alta Disponibilidad.
    - Esto implica el uso de configuraciones Activo-Pasivo o Activo-Activo con replicación síncrona o asíncrona de datos en tiempo real entre los nodos.
    - Si el nodo principal de la base de datos falla (ej. por corrupción o fallo de hardware), el clúster debe ejecutar una Conmutación por Error (Failover) automática y transparente al nodo secundario en cuestión de segundos, garantizando un RTO extremadamente bajo (Capítulo 9.4.1).

- **Balanceo de carga (load balancing) y servidores de aplicación redundantes:**
    - Los servidores de aplicación (donde reside la lógica de negocio y los workflows) deben ser redundantes y modulares.
    - Todos los servidores de aplicación deben operar detrás de un Balanceador de Carga (Load Balancer) que distribuye las peticiones de los usuarios. Si un servidor de aplicación falla, el Balanceador de Carga lo detecta y redirige automáticamente todo el tráfico a los servidores funcionales restantes, manteniendo la continuidad del servicio sin intervención manual.

- Almacenamiento redundante y tolerancia a fallos del repositorio:
    - El Repositorio de Archivos Binarios (la capa de almacenamiento de los documentos) debe utilizar tecnologías inherentemente tolerantes a fallos, como la configuración RAID (Redundant Array of Independent Disks) a nivel local o, preferentemente, Almacenamiento de Objetos con Replicación Inherente (Modelo Híbrido Capítulo 9.1.3).
    - Esta redundancia asegura que la falla de un disco o de una unidad de almacenamiento no resulte en la pérdida de documentos, garantizando la disponibilidad física inmediata de los archivos.

- Monitoreo de componentes de HA:
    - Es fundamental implementar el monitoreo continuo 24/7 de la salud de todos los componentes de HA (estados de replicación, latencia del failover y carga del Balanceador), asegurando que los mecanismos de redundancia estén siempre listos para operar en caso de un incidente.

9.4.4. Plan de recuperación ante desastres (DRP):

El Plan de Recuperación ante Desastres (DRP) es un documento formal, obligatorio y ejecutable que debe ser creado y mantenido bajo la Gobernanza Técnica de la Alcaldía. Su propósito es detallar, paso a paso, el procedimiento técnico y administrativo para activar el sitio de contingencia (DR Site) y restaurar la operación del SGDEA en un tiempo que no exceda el RTO (Objetivo de Tiempo de Recuperación) definido en el BIA (Capítulo 9.4.1).

- Gobernanza y Roles y Responsabilidades (BCP):
    - El DRP debe definir una Estructura de Comando y Control clara. Se deben asignar formalmente los Roles y Responsabilidades del Equipo de Recuperación (liderazgo, equipo de TI, equipo de archivo/funcional) con sus datos de contacto actualizados y la cadena de escalamiento.
    - Este equipo es responsable de ejecutar el plan y de tomar las decisiones críticas durante la emergencia.

- Criterios y Declaración de Desastre:

    - El plan debe establecer Criterios Claros y Medibles para la Declaración Formal de Desastre, incluyendo la duración de la interrupción del servicio, el alcance del daño a la infraestructura o la violación del SLA (Capítulo 9.3.1).
    - Se debe identificar la Autoridad Designada (ej. Jefe de TI o Gerente del Proyecto SGDEA) que tiene la potestad exclusiva para declarar el desastre y autorizar la activación del DR Site.

- Procedimientos Técnicos de Activación (Cumplimiento de RPO):
    - Se detallarán los Procedimientos Técnicos pormenorizados para levantar la infraestructura del SGDEA en el sitio alterno. Esto incluye:
        1. Validación del último RPO (punto de pérdida de datos).
        2. Activación de los recursos de cómputo y red del DR Site.
        3. Restauración o sincronización de las Bases de Datos (metadatos) y del Repositorio de Archivos Binarios desde la copia de respaldo o réplica.
        4. Pruebas funcionales de criticidad (ej. radicación exitosa, acceso a documentos).

- Plan de Comunicación y Documentación Legal:
    - Es fundamental un Plan de Comunicación que especifique a quién, cuándo y cómo se debe informar sobre la indisponibilidad y el estado de la recuperación (usuarios finales, directivos, entes de control, y ciudadanos).
    - Se debe incluir el procedimiento para documentar legalmente la declaración de desastre y la activación del sitio alterno, preservando los *logs* de eventos y las acciones tomadas para futuras auditorías.

- Procedimiento de Retorno a la Operación (*Failback*):
    - El DRP debe incluir un plan detallado para el Retorno a la Operación (*Failback*) al sitio principal una vez que la emergencia haya sido superada y el sitio primario haya sido restaurado y validado.
    - El *Failback* es un procedimiento crítico que requiere la replicación inversa de todos los datos generados en el sitio alterno hacia el sitio principal, minimizando la ventana de riesgo de una nueva interrupción.

- Pruebas y Mantenimiento del DRP:
    - El DRP es un documento vivo. Es obligatorio realizar simulacros y pruebas de DRP de forma periódica (mínimo semestral o anualmente) para validar la efectividad de los procedimientos y el cumplimiento de los RTO/RPO. El DRP debe ser revisado y actualizado después de cada prueba fallida o después de cualquier cambio significativo en la arquitectura del SGDEA

9.5. Arquitectura de seguridad y ciber-resiliencia

La seguridad del SGDEA no es una funcionalidad opcional, sino un imperativo legal y archivístico (alineado con ISO/IEC 27001 y los requisitos de autenticidad e integridad del AGN). El diseño de la arquitectura debe ser intrínsecamente ciberresiliente, implementando un modelo de Defensa en Profundidad (Defense in Depth) en cada capa del sistema, desde la red hasta el dato.

- Modelo de Seguridad por Capas (Defense in Depth):
    - La arquitectura debe implementar controles de seguridad en múltiples niveles: Perímetro de red (firewalls y segmentación), Aplicación (WAF, validación de inputs) y Datos (cifrado y control de acceso RBAC), asegurando que una falla en un componente no comprometa la integridad de los documentos.
    - Segmentación de Red: Se exige la segmentación de red entre el ambiente transaccional (alta actividad) y el repositorio de preservación (alta inmutabilidad), limitando el acceso solo a los servicios esenciales.

- Cifrado Obligatorio y Gestión de Claves:
    - Cifrado en Reposo (At-Rest): Todos los documentos electrónicos y los metadatos almacenados en bases de datos y repositorios deben estar cifrados en reposo utilizando algoritmos robustos (ej. AES-256).

- Cifrado en Tránsito (In-Transit): Toda la comunicación interna (entre servidores) y externa (con usuarios o APIs) debe utilizar protocolos seguros y actualizados (TLS 1.2 o superior).
- Gestión de Claves (KMS): El sistema debe utilizar un Sistema de Gestión de Claves (KMS) centralizado y seguro para la administración de las claves de cifrado, asegurando que las claves estén separadas de los datos que cifran y bajo estricto control.

- Autenticación Reforzada y Gestión de Identidades (IAM):

  - Autenticación Multifactor (MFA): La Autenticación Multifactor (MFA) será obligatoria para todos los administradores del sistema, los usuarios con privilegios elevados (ej. Jefes de Archivo) y el acceso a la infraestructura crítica (Capítulo 9.3.1).
  - Conexión a Directorio Central: El SGDEA debe integrarse al Sistema de Gestión de Identidades (IAM) central de la Alcaldía (ej. Active Directory) para la autenticación única (SSO), utilizando el Modelo RBAC para la asignación de permisos con el principio de Mínimo Privilegio.

- Pruebas de Ciber-resiliencia:
  - Se exigirá la realización de Pruebas de Penetración (Penetration Testing) y Análisis de Vulnerabilidades por parte de un tercero independiente al menos una vez al año, o antes de cada despliegue mayor, para identificar y mitigar proactivamente las debilidades de la arquitectura y el código

9.6. Matriz de asignación arquitectónica y riesgo (MAAR)

Esta matriz es esencial para la toma de decisiones final y para formalizar la Gobernanza Técnica del SGDEA. Su propósito es vincular cada componente funcional del sistema con su ubicación física, sus requisitos de resiliencia y su nivel de criticidad legal/operacional. Esto traduce las políticas de BIA/DRP y el Modelo Híbrido en un plan de despliegue ejecutable.

Conceptos	Descripción y Propósito	Capítulo Relacionado
Componente del SGDEA	Define la unidad funcional o lógica: Motor de Radicación, Base de Datos Metadatos Transaccionales, Repositorio de Preservación Histórica, Motor de Workflows, Portal VUE/APIs.	8.2, 8.3
Clasificación de Criticidad (BIA)	Nivel de impacto de su indisponibilidad: Crítico Legal (fe pública), Crítico Operacional (flujos de trabajo), Alto (acceso ciudadano).	9.4.1 (BIA)
Modelo de Despliegue Propuesto	Asignación estratégica de la ubicación física: Local (On-Premise), Nube Privada (Soberanía Controlada) o Nube Pública (Elasticidad).	9.1 (Modelo Híbrido)
RPO Objetivo	Pérdida máxima de datos aceptable (ej. 15 min, 4 horas). Define la frecuencia de replicación/respaldo.	9.4.2001
RTO Objetivo	Tiempo máximo de inactividad aceptable (ej. 4 horas, 8 horas). Define el tiempo de Failover / Recuperación.	9.4.2001

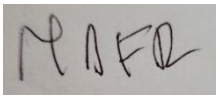
Conceptos	Descripción y Propósito	Capítulo Relacionado
Requisito Clave de Seguridad/HA	Especifica la tecnología requerida para la capa (ej. HA Activo-Activo, Cifrado At-Rest, Tecnología WORM, MFA Obligatorio).	9.4.3 (HA), 9.5 (Seguridad)

10. Ficha Técnica.

Campo	Descripción
Título del Documento	Desarrollo, funcionales clave y diseño preliminar de arquitectura tecnológica de un sistema de gestión de documentos electrónicos de archivo SGDEA
Sumario	Definición de los procesos del ciclo de vida documental que debe gestionar el sistema, controles requeridos de integridad, accesibilidad y trazabilidad documental, requisitos para la interfaz administrativa (perfiles, control de versiones, reportes, etc.), Lineamientos para el almacenamiento seguro de documentos electrónicos, Requerimientos de interoperabilidad con sistemas institucionales (como SIGEP, SECOP, ORFEO, etc.). Recomendaciones para la gestión de patrimonio digital y preservación a largo plazo. Evaluación comparativa: implementación en la nube vs. infraestructura local. Definición de requerimientos mínimos de escalabilidad (1 TB inicial), especificaciones del modelo de soporte postimplementación (recomendado: 24/7 mínimo 6 meses). Consideraciones de continuidad operativa, respaldo y recuperación.
Palabras Clave	Gestión Documental Electrónica (GDE), Ciclo de Vida, la Seguridad (Integridad, Trazabilidad, Accesibilidad), la Interoperabilidad, la Preservación Digital, Escalabilidad, Continuidad Operativa, comparativa Nube vs. Local, normatividad colombiana (AGN, SIGEP, SECOP, ORFEO) y estándares como ISO 15489 para los requisitos funcionales y técnicos del sistema.
Formato	PDF (versión oficial entregable)
Código Interno	
Lenguaje	Español
Entidad	Alcaldía Mayor de Cartagena de Indias – Dirección

Campo	Descripción
Contratante	Administrativa del Archivo General del Distrito
Contratista – Ejecutor Técnico	Unión Temporal GDE Soluciones 2025
Objeto del Contrato Asociado	Elaboración del Diagnóstico Integral de Archivos y del Modelo de Requisitos para la Implementación del Sistema de Gestión de Documentos Electrónicos de Archivo – SGDEA
Etapa Ejecutad	Planeación y Diseño del Sistema
Versión del Documento	1.0
Estado	Aprobado para entrega contractual
Revisó	Dirección Administrativa del Archivo General del Distrito
Validó	Supervisor del Contrato CMA-SEGD-004-202
Lugar de Emisión	Cartagena de Indias, Distrito Turístico y Cultura

Rol	Nombre/Cargo	Firma	Fecha
Director del Proyecto – UT GDE Soluciones 2025	Huver Nieto Gómez – Director del Proyecto – UT GDE Soluciones 202		**17/12/2025**

Coordinador del Proyecto– **UT GDE Soluciones 2025**	Miguel Forero - Coordinador del proyecto - UT GDE Soluciones		**17/12/2025**
Supervisor del Contrato **CMA-SEGD-0**	José Carlos Puello Rubio – Director Administrativo del Archivo General del Distrito