DEPARTAMENTO DE BOLÍVAR

GOBERNACIÓN DE BOLÍVAR

SECRETARIA GENERAL
DIRECCIÓN DE ATENCIÓN AL CIUDADANO Y GESTIÓN DOCUMENTAL

MODELO DE REQUISITOS PARA LA GESTIÓN DE DOCUMENTOS ELECTRÓNICOS

TURBACO - BOLIVAR
NOVIEMBRE DE 2021

Tabla de contenido

INTRODUCCIÓN---------- 4

1. GENERALIDADES---------- 6

1.1. PROPÓSITO ---------- 6

1.2. ALCANCE ---------- 6

1.3. OBJETIVOS ---------- 6

1.3.1. Objetivo General. ---------- *6*

1.3.2. Objetivos Específicos. ---------- *6*

1.4. GLOSARIO ---------- 7

1.5. MARCO NORMATIVO ----------13

1.6. DOCUMENTOS ASOCIADOS----------15

2. MODELO DE REQUISITOS----------16

2.1. CANALES DE COMUNICACIÓN DE LA GOBERNACIÓN DE BOLÍVAR ----------16

2.2. ESQUEMA GENERAL DEL MANEJO DE DATOS EN EL SISTEMA DE GESTIÓN DOCUMENTAL ---------16

2.3. SISTEMA DE GESTIÓN DE DOCUMENTOS ELECTRÓNICOS----------17

2.3.1. Requisitos Funcionales. ----------*18*

2.3.1.1. Requisitos Funcionales de Configuración del SGDEA. ----------18

2.3.1.2. Requisitos Funcionales de Creación e Ingreso de Documentos del SGDEA. ------22

2.3.1.3. Requisitos Funcionales de Clasificación, Organización, Retención y Disposición Final en el SGDEA.----------24

2.3.1.4. Requisitos de Búsqueda, Recuperación y Reproducción. ----------27

2.3.1.5. Requisitos Funcionales de Acceso, Seguridad, Controles de Acceso, Controles de Seguridad y Niveles de Seguridad del SGDEA. ----------29

2.3.1.6. Requisitos Funcionales de Ejecución de Controles de Seguridad y Categorías de Seguridad del SGDEA.----------31

2.3.1.7. Requisitos Funcionales de Gestión de Metadatos del SGDEA. ----------33

2.3.1.8. Requisitos Funcionales de Flujos de Trabajo del SGDEA. ----------34

2.3.2. Requisitos No Funcionales.----------*36*

2.3.3. Requerimientos Complementarios. ----------*38*

2.3.3.1. Management of Physical (Non-electronic) files and Records, and Disposition of Physical Records - Administración física de registros, documentos y disposición final de los mismos (conservación).----------38

2.3.3.2. Workflow- Flujos de Trabajo ----------39

2.3.3.3. Requisitos técnicos y operativos adicionales del Sistema ----------39

Tabla de Figuras

Figura 1: Canales comunicación Gobernación de Bolívar----------16

Figura 2: Esquema de manejo de datos e información Institucional----------17

INTRODUCCIÓN

La modernización administrativa en las Entidades del Estado ha generado diferentes avances encaminados al mejoramiento de la atención efectiva y eficiente de sus grupos de interés, respondiendo a las nuevas necesidades y requerimientos del contexto contemporáneo del país.

Esto se ve reflejado y ligado con los avances tecnológicos en todos los procesos gestionados, en donde específicamente en la Gestión documental la concepción del significado de documento se ha desarrollado de acuerdo con el medio de recibo, ya no solo manejado en papel sino introduciendo el concepto de documento electrónico como base.

Así mismo, llevando este documento electrónico a la perspectiva de un documento Electrónico de Archivo el cual cumple con unas características específicas que garantizan la conservación y preservación del acervo documental de la **Gobernación de Bolívar**, convirtiéndose como documento público en la evidencia y soporte de los principios de transparencia y acceso a la información a los grupos de interés de acuerdo a lo establecido en la Ley 1712 de 2014 y los lineamientos dados para tal fin por el Archivo General de la Nación.

Esta propuesta de requerimientos funcionales y No funcionales son los que debería cumplir el Sistema de Gestión de Documentos Electrónicos de Archivo, convirtiéndose este en pieza clave de la Arquitectura de Información.

Mediante la promulgación de la Ley 594 del 2000, se establece la función archivística de las entidades públicas, a través de esta que se efectúa la reglamentación de los diversos procesos documentales de las Entidades, en tal sentido es pertinente garantizar el fortalecimiento de los sistemas de información, enmarcados en el desarrollo de las nuevas tecnologías de la información y las comunicaciones.

Con fundamento en la orientación que los sistemas de archivo y gestión documental se han convertido en dependencias estratégicas que brindan funciones de apoyo tanto para el desarrollo de las actividades misionales de las Organizaciones, como de mecanismo facilitador en la garantía de los derechos, alineados con los objetivos nacionales de Lucha contra la corrupción, transparencia y rendición de cuentas.

En ese orden de ideas el Ministerio de Cultura, junto con el Ministerio de las Tecnologías y las Comunicaciones (MINTIC), en armonía con el Archivo General de la Nación, en especial lo dispuesto por medio del Decreto 2609 de 2012, recopilado en el Decreto único reglamentario del sector cultura, Decreto 1080 de mayo 26 de 2015, Capitulo VII, norma mediante la cual se procedió a reglamentar los requisitos para la gestión de documentos electrónicos y los Sistema de Gestión Documental en las Entidades Públicas, así mismo incorporó el Modelo de Requisitos Para la Gestión de Documentos Electrónicos como el instrumento archivístico que desarrolla el presente capitulo.

Igualmente, se tuvieron en cuenta normas internacionales para fortalecer la identificación de requisitos que apoyen la gestión de los documentos electrónicos de archivo, tales como la Norma ISO 15489-1, 16175-2. Además, se contempló la normatividad legal colombiana como contexto general, y la capacidad institucional de mejorar procesos y poder concluir con resultados reales en el mediano y largo plazo.

El presente documento establece el modelo de requerimientos funcionales que deben cumplir los documentos electrónicos como resultado del ejercicio de Planeación y Análisis preliminar y que tuvo como referencia la Guía del Archivo General de la Nación - AGN denominada “Implementación de un Sistema de Gestión de Documentos Electrónicos de Archivo”, en el que se establece a modo general, la necesidad de estructurar una estrategia de integración de sistemas de gestión que facilite la aplicabilidad y control de cada una de las etapas de la gestión de documentos (creación, mantenimiento, difusión y administración).

En consecuencia, con lo anteriormente expuesto, se procede a efectuar mediante este documento una serie detallada de recomendaciones, con el propósito de facilitar la adecuada normalización y el cumplimiento de los estándares de la gestión documental electrónica en la **Gobernación de Bolívar**.

1. GENERALIDADES

1.1. Propósito

Establecer los requisitos mínimos para la Implementación de un sistema de información para los procesos de gestión documental y atención a grupos de interés que integre las fuentes de información y los servicios que apoyan los procesos de gestión, logrando el flujo continuo y de calidad de la información que requiere la **Gobernación de Bolívar** para prestar sus servicios y cumplir sus funciones, estableciendo los lineamientos básicos para el desarrollo del Sistema de Gestión de Documentos Electrónicos de Archivo en la entidad que contribuya a optimizar su gestión, satisfaga las necesidades de información y la prestación de servicios hacia las poblaciones beneficiarias en el territorio.

1.2. Alcance

La implementación de un gestor documental se constituye un marco de acción para las decisiones en materia de Gestión de Documentos, Gestión de Registros, Gestión de contenido en general para las decisiones en materia de automatización de la administración de los activos de información de la **Gobernación de Bolívar** con el objetivo final de contribuir a la eficacia organizacional, aplicable a los procesos de la entidad, a personas y actividades que involucran directa o indirectamente el manejo de documentos físicos y electrónicos y en general el contenido generado y recibido en ejercicio de las funciones propias institucionales.

La solución tecnológica de gestión de contenidos optimizara la estrategia de manejo de documentos y registros, el desarrollo de la cultura de gestión bajo un modelo de manejo documental integrado y escalable, logrando la alineación para la administración eficiente de los contenidos institucionales, con la estrategia corporativa, la gestión de relación con los grupos de influencia o interés y el logro de acceso con calidad a fuentes de información de manera confiable y oportuna.

1.3. Objetivos

1.3.1. Objetivo General.

Estructurar la estrategia para la producción de documentos electrónicos, la integración e interoperabilidad de los sistemas de gestión que tiene la **Gobernación de Bolívar** para facilitar la aplicabilidad y control de cada una de las etapas de la gestión de documentos: creación, mantenimiento, difusión y administración.

1.3.2. Objetivos Específicos.

- Automatizar y soportar los procesos de la Entidad y la información producida o generada en las diferentes oficinas productoras a nivel funcional.
- Permitir la clasificación de los documentos que ingresan, transfieren y salen de la **Gobernación de Bolívar** en diferentes niveles de responsabilidad, iniciando de lo

general a lo particular; es decir, que los servidores de ventanilla reciban y clasifiquen un primer nivel con el conocimiento básico del área competente para gestionar la solicitud (series y dependencias) y en un segundo nivel la dependencia encargada de dar respuesta para clasificarlo por subserie y tipo documental, realizando filtros de acuerdo a los tipos documentales que maneja cada dependencia, y de esta forma obtener informes detallados de la información que maneja la **Gobernación de Bolívar**, por tipo documental, subserie, serie.

- Reducir de manera significativa los errores de clasificación por series y subseries.
- Reducir los errores de enrutamiento a las diferentes dependencias.
- Administrar los diferentes canales de comunicación (presencial, redes sociales, fax, correos electrónicos institucionales, telefónico, escrito).
- Gestionar expedientes electrónicos.
- Automatizar el procedimiento del módulo de notificaciones para los actos administrativos que expide la **Gobernación de Bolívar**, de acuerdo con la Ley 1437 de 2011, incluidas todas aquellas que adicionen, modifiquen o deroguen durante la implementación.
- Permitir la creación y gestión de documentos electrónicos y digitalizados con firma digital.

1.4. Glosario

Términos tomados de las siguientes fuentes: Manual para implementación de Política Gobierno Digital V5, Acuerdo 027 de 2006 AGN, Decreto 1078 de/2015, Guía Implementación SGDEA - AGN, NTC-ISO 16175-3, Decreto 2609 de 2012, Ley 1712 de 2014, Acuerdo 003 /2015, Marco de Referencia - Arquitectura TI, Ley 527 de1999:

- **Acceso**. Proceso de recuperación y visualización (presentación) de documentos electrónicos (y físicos) con fines operativos, históricos o como evidencia.
- **Accesibilidad**. Es una característica deseable en las páginas web e interfaces gráficas de los sistemas de información que consiste en la posibilidad que tiene un usuario de acceder a un sitio web y navegar en él, sin importar que cuente con algún tipo de discapacidad. Esto de acuerdo con la caracterización de usuarios, ciudadanos y grupos de interés de la entidad.
- **Almacenamiento de documentos**. Acción de guardar sistemáticamente documentos de archivo en espacios, mobiliario y unidades de conservación apropiadas.
- **Análisis de Brecha**. Se refiere a la identificación, comparación y análisis de las diferencias entre un estado o situación actual y el estado o situación deseada. Permite planear las arquitecturas de transición necesarias para implementar y alcanzar la arquitectura empresarial objetivo.
- **Archivo electrónico**. Conjunto de documentos electrónicos producidos y tratados conforme a los principios y procesos archivísticos.
- **Arquitectura Empresarial**. Es una práctica estratégica que consiste en analizar integralmente las entidades desde diferentes perspectivas o dimensiones, con el propósito de obtener, evaluar y diagnosticar su estado actual y establecer la

transformación necesaria. El objetivo es generar valor a través de las TIC para que se ayude a materializar la visión de la entidad.

- **Autenticidad**. Característica técnica para preservar la seguridad de la información que busca asegurar la validez en el tiempo, forma y distribución. Así mismo, garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- **Autenticación**. Proceso de probar una aseveración a fin de establecer un nivel de confianza en la veracidad de dicha aseveración.
- **Autenticación Electrónica**. Es la acreditación por medios electrónicos de la identidad de una persona o autoridad, para elaborar o firmar documentos, o para adelantar trámites y procedimientos administrativos.
- **Autoridad de disposición**. Instrumento formal que define los períodos de retención y acciones de disposición consecuentes autorizadas para clases de registros descritos en dicho documento.
- **Captura de documentos de archivo**. Incorporación del documento al SGDEA. Incluye el registro, clasificación, asignación de metadatos y su almacenamiento. Los documentos elaborados o recibidos en el curso de la actividad se convierten en documentos de archivo cuando se guardan, esto es, “se capturan” en el SGDEA. En esta captura se clasifican, es decir, se le asignan códigos que hacen referencia a la clase a la que pertenecen.
- **Código**. Identificación numérica o alfanumérica que se asigna tanto a las unidades productoras de documentos y a las series y subseries respectivas, y que debe responder al sistema de clasificación documental establecido en la entidad.
- **Conservación de documentos**. Conjunto de medidas preventivas o correctivas adoptadas para asegurarla integridad física y funcional de los documentos de archivo.
- **Conservación preventiva de documentos**. Conjunto de estrategias y medidas de orden técnico, político y administrativo orientadas a evitar o reducir el riesgo de deterioro de los documentos de archivo, preservando su integridad y estabilidad.
- **Contenido estable**. El contenido del documento no cambia en el tiempo: los cambios deben estar autorizados conforme a reglas establecidas, limitadas y controladas por la entidad, o el administrador del sistema, de forma que, al ser consultado cualquier documento, una misma pregunta, solicitud o interacción genere siempre el mismo resultado.
- **Controles de acceso**. Esquemas de mecanismos no jerárquicos, que se pueden aplicar a registros digitales para prevenir el acceso de usuarios no autorizados. Puede incluir la definición de grupos con acceso de usuarios y listas ad hoc de usuarios identificados de forma individual.
- **Copia**. Reproducción exacta de un documento.
- **Copia autenticada**. Reproducción de un documento, expedida y autorizada por el funcionario competente y que tendrá el mismo valor probatorio del original.
- **Componente**. Conjunto de elementos constitutivos que conforman un registro digital, (tales como los componentes multimedia de una página web). Se hace necesario capturar metadatos acerca de componentes para posibilitar que un

registro se gestione con el paso del tiempo, por ejemplo, para propósitos de migración. Esto no se debe confundir con el concepto de componente de "software" o "sistema".

- **Clase**. Parte de una jerarquía representada por una línea que va desde cualquier punto del cuadro jerárquico de clasificación a todos los expedientes que quedan por debajo.
- **Conformación de expedientes electrónicos de archivo**. El expediente electrónico de archivo se conformará con la totalidad de los documentos de archivo generados en desarrollo de un mismo trámite, actuación o procedimiento, independientemente del tipo de información y formato, y deben agruparse formando series o subseries documentales. Adicionalmente, atenderán las series documentales establecidas en los cuadros de clasificación documental adoptados por cada entidad, desde el primer momento en que se inicia un trámite o procedimiento hasta la finalización de este, abarcando los documentos (independientemente de su soporte) que se generen durante la vigencia y prescripción de las acciones administrativas, fiscales y legales.
- **Cierre y Archivo del expediente electrónico**. Cuando finalice la actuación o procedimiento administrativo, la autoridad deberá cerrar el expediente y firmar el índice. Se deberán utilizar mecanismos electrónicos seguros, para garantizar la integridad, autenticidad y disponibilidad en el tiempo de manera que no puedan ser modificados, eliminados o reemplazados conforme a los lineamientos tecnológicos establecidos por la entidad, y los lineamientos archivísticos establecidos por el Archivo General de la Nación. Cuando el expediente se archive, se debe generar o convertir en un formato que permita asegurar su autenticidad, integridad, recuperación, conservación y preservación a mediano y largo plazo, conforme a los criterios de valoración documental establecidos por el Archivo General de la Nación y los lineamientos tecnológicos establecidos por la **Gobernación de Bolívar**.
- **Datos abiertos**. Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.
- **Digitalización**. Técnica que permite la reproducción de información que se encuentra guardada de manera analógica (soportes, papel, video, casettes, cinta, película, microfilm otros) en una que sólo puede leerse o interpretarse por computador.
- **Documento o registro electrónico**. Registro digital o electrónico, generado y autorizado; enviado, recibido, capturado, clasificado, indexado o almacenado por medios electrónicos o similares y/o sujeto de algún otro proceso archivístico, que incluya (el registro) equivalente funcional y niveles aceptables de autenticidad, fiabilidad, integridad y usabilidad. Atributos similares a las características de: Contenido estable, Forma documental fija, Vinculo Archivístico (Elaboración mesa técnica SGDEA).

- **Documento electrónico de archivo**. Los documentos electrónicos serán de archivo cuando por su valor administrativo, fiscal, legal, científico, histórico, técnico o cultural, adquieran esa naturaleza. En cuyo caso, deberán ser tratados conforme a los principios y procesos archivísticos, y permanecer almacenados electrónicamente durante todo su ciclo de vida.
- **Disponibilidad de los documentos electrónicos de archivo**. Los documentos electrónicos de archivo se podrán a disposición de las personas interesadas en formatos que permitan de forma gratuita la lectura, comprobación de la firma electrónica y el descifrado, sin perjuicio de las disposiciones legales de reserva legal, en concordancia con lo reglamentado en la Ley 1712 de 2014.
- **Documento esencial**. Documento necesario para el funcionamiento de un organismo y que, por su contenido informativo y testimonial, garantiza el conocimiento de las funciones y actividades de este, aun después de su desaparición, por lo cual posibilita la reconstrucción de la historia institucional.
- **Expediente electrónico:** El expediente electrónico se creará cuando los documentos electrónicos tengan la naturaleza de archivo.
- **Expediente electrónico de archivo**. Conjunto de documentos y actuaciones electrónicos producidos y recibidos durante el desarrollo de un mismo trámite o procedimiento, acumulados por cualquier causa legal, interrelacionados y vinculados entre sí, manteniendo la integridad y orden dado durante el desarrollo del asunto que les dio origen y que se conservan electrónicamente durante todo su ciclo de vida, con el fin de garantizar su consulta en el tiempo.
- **Elementos del Expediente electrónico de archivo**. El expediente electrónico tendrá como mínimo los siguientes elementos: 1.) Documentos e electrónicos de archivo; 2.) Foliado electrónico; 3.) índice electrónico; 4.) firma del índice electrónico; 5.) Metadatos o información virtual contenida en ellos.
- **Firma Digital**. Mecanismo de seguridad incluido dentro de un registro digital que posibilita la identificación del creador del objeto digital y que también puede emplearse para detectar y rastrear cualquier cambio que se haya realizado al objeto digital.
- **Firma electrónica**. Las firmas electrónicas (en este caso, firmas digitales) consisten en información que se adjunta o está asociada lógicamente con otra información, como un registro electrónico, y que sirve como método de autenticación. La firma electrónica normalmente toma la forma de una secuencia de caracteres. Se utiliza con algoritmos, procedimientos y “claves” seguras (una larga cadena de caracteres análogos a una contraseña) para confirmar la integridad de un registro y / o para autenticar la identidad del remitente o la fuente de un registro. Las firmas electrónicas no deben confundirse con un mapa de bits, o imagen escaneada, de una firma manual de "pluma y tinta" en el papel; esto no se considera seguro y, por lo tanto, es poco probable que se agregue a la evidencia sobre la autenticidad de un registro. Una firma electrónica, como se usa el término en MoReq2, es una forma de "firma electrónica avanzada" tal como se define en la "Directiva europea sobre un marco comunitario para las firmas electrónicas" 1999/93 / EC. Una firma electrónica avanzada es aquella que cumple con la definición de la Directiva, a saber, que la firma está: vinculada únicamente al firmante; • capaz de identificar al firmante; • creada mediante

medios que el firmante puede mantener bajo su control exclusivo; • vinculada a los datos (por ejemplo, registro) con los que se relaciona de tal manera que cualquier cambio posterior de los datos (por ejemplo, registro) sea Detectable.

- **Foliado electrónico.** Asociación de un documento electrónico a un índice electrónico en un mismo expediente electrónico o serie documental con el fin de garantizar su integridad, orden y autenticidad.
- **Foliado electrónico de archivo y características**. Los documentos electrónicos de archivo que conforman el expediente electrónico de archivo deben ser foliados. El foliado debe incluir dentro de sus atributos la numeración consecutiva de los documentos que conforman el expediente o la serie documental simple, y atender los principios archivísticos que dicte el Archivo General de la Nación.
- **Gobierno de Arquitectura Empresarial**. Es una práctica orientada a establecer instancias de decisión, alinear los procesos institucionales o de negocio con los procesos, recursos y estrategias de TI, para agregar valor a las organizaciones y apoyar el cumplimiento de sus objetivos estratégicos. El gobierno de Arquitectura empresarial gestiona y controla los riesgos, mide el desempeño de la arquitectura, define políticas de arquitectura, gestiona la evolución y cambios sobre los artefactos o productos de la arquitectura. El gobierno de la arquitectura es parte del gobierno corporativo o empresarial.
- **Integridad**. se refiere a la garantía de que una información no ha sido alterada, borrada, reordenada, copiada, etc., bien durante el proceso de transmisión o en su propio equipo de origen.
- **Intercambio electrónico de datos**. La transmisión electrónica de datos de una computadora a otra, que está estructurada bajo normas técnicas convenidas al efecto.
- **Medio electrónico**. Mecanismo tecnológico, óptico, telemático, informático o similar, conocido o por conocerse que permite producir, almacenar o transmitir documentos, datos o información.
- **Metadatos**. Información estructurada que describe y/o permite a los usuarios hallar, gestionar, controlar, comprender o preservar otra información con el paso del tiempo.
- **Metadatos de Registros**. Información que Identifica, autentica y contextualiza los registros y personas, procesos y sistemas que los crean, administran, mantienen y los utilizan, y las políticas que los gobiernan.
- **Migración**. Acto de mover registros de un sistema a otro, al tiempo que se mantiene la autenticidad, integridad, confiabilidad y usabilidad de los registros. La migración incluye un conjunto de tareas organizadas diseñadas para transferir de forma periódica material digital de una configuración de hardware o software a otra, o de una generación de tecnología a otra.
- **Microfilmación**. Técnica que permite registrar fotográficamente documentos como pequeñas imágenes en película de alta resolución.
- **Rastreo (tracking)**. Creación, captura y mantenimiento de información acerca del movimiento y uso de los registros.

- **Registro Digital**. Registros en medios de almacenamiento digital, producidos, comunicados, mantenidos y/o a los que se tiene acceso por medio de equipo digital.
- **Registro o Documento electrónico (RDE)**. Registro digital o electrónico, generado y autorizado; enviado, recibido, capturado, clasificado, indexado o almacenado por medios electrónicos o similares y/o sujeto de algún otro proceso archivístico, que incluya (el registro) equivalente funcional y niveles aceptables de autenticidad, fiabilidad, integridad y usabilidad. Atributos similares a las características de: Contenido estable, Forma documental fija, Vinculo Archivístico.
- **Repositorios digitales confiables de expedientes electrónicos**. Las autoridades y las empresas que presenten servicios de archivo electrónico a entidades públicas deberán garantizar la utilización de repositorios digitales confiables, para la preservación a largo plazo de los documentos y expedientes electrónicos de archivo de acuerdo con los tiempos de conservación establecidos en la Tabla de Retención Documental, mientras se encuentren bajo su custodia y deberán garantizar como mínimo: 1.) El acceso a largo plazo de los documentos electrónicos de archivo producidos por las autoridades; 2.) El monitoreo, planeación y mantenimiento de todos los documentos electrónicos de archivo generados; 3.) El mantenimiento, así como la estrategia para la implementación de programas de preservación a largo plazo.
- **Sistema de Gestión Documental Electrónico de Archivo (SGDEA)**. es una herramienta informática destinada a la gestión de documentos electrónicos de archivo. También se puede utilizar en la gestión de documentos de archivo tradicionales.
- **Sistema de Información**. Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.
- **Sistema de Gestión de Registros Electrónicos (ERMS)**. Sistema automatizado empleado para gestionar la creación, uso, mantenimiento y disposición de registros creados de forma digital con el fin de brindar evidencia de las actividades de negocio. Estos sistemas mantienen información contextual apropiada (metadatos) y vínculos entre registros para soportar su valor como evidencia.
- **Transferencias secundarias de documentos y expedientes electrónicos**. Las autoridades y entidades públicas, así como las entidades privadas que cumplen funciones públicas, deberán dar cumplimiento a lo establecido en el Decreto 1515 de 2013, en cuanto a la obligación de realizar las transferencias secundarias de documentos electrónicos de valor permanente al Archivo General de la Nación o a los Archivos Generales Departamentales, Distritales y Municipales, según su competencia, y cumplir los requisitos establecidos por el Archivo General de la Nación en esta materia.
- **Usabilidad**. Un registro usable es aquel que se puede ubicar, recuperar, presentar e interpretar dentro de un periodo de tiempo considerado razonable por las partes interesadas. Un registro usable debería estar conectado al proceso de transacción de negocio que lo produjo. Se deberían conservar los vínculos entre los registros que documentan las transacciones de negocio relacionadas.

- **Valoración documental**. Labor intelectual por la cual se determinan los valores primarios y secundarios de los documentos con el fin de establecer su permanencia en las diferentes fases del ciclo vital.

1.5. Marco Normativo

A continuación, se referencian la normatividad relevante tomada en cuenta en el desarrollo del presente documento:

- **Ley 594 de 2000**: "Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones".
- **Acuerdo 038 de 2002**: "Por el cual se desarrolla el artículo 15 de la Ley General de Archivos 594 de 2000".
- **ISO/TR 26122:2008**. Work Process analysis for records: Informe técnico que proporciona orientaciones sobre el análisis de procesos de trabajo desde la perspectiva de la creación, captura y control de los documentos. Identifica dos tipos de análisis: I. análisis funcional (Descomposición de las funciones en procesos), y II. Análisis secuencial (investigación del flujo de transacciones).
- **ISO 42010**: Sistemas e Ingeniería de software, descripción de la arquitectura define los requisitos que debe cumplir las descripciones que se hagan de arquitecturas empresariales, de sistemas o de software.
- **UNE-ISO 30301:2011**- Sistemas de Gestión documental: Norma especialmente útil para demostrar la conformidad con los requisitos de control de documentos.
- **Ley 1581 de 2012**: Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Decreto 2609 de 2012** "Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado."
- **UNE-ISO 16175-1:2012 / UNE-ISO 16175-2:2012** /: Norma que establece en sus tres partes los principios de buenas prácticas mediante una propuesta de directrices que deben cumplir el sistema y la organización, y una propuesta de requisitos funcionales que debe cumplir el software que controlará el sistema de gestión de los documentos en un entorno de oficina electrónica. Parte1: Generalidades y declaración de principios; Parte2: Directrices y requisitos funcionales para sistemas que gestionan documentos electrónicos; Parte3: Directrices y requisitos funcionales para documentos en los sistemas de la organización.
- **NTC-ISO 30301:2013** Información y Documentación. Sistemas de Gestión de Registros. Requisitos. Esta norma específica, los requisitos que un Sistema de Gestión de Registros debe cumplir.
- **Acuerdo 006 de 2014**: "Por medio del cual se desarrollan los artículos 46, 47 y 48 del Título XI "Conservación de Documentos" de la Ley 594 de 2000".
- **Ley 1712 del 6 de marzo de 2014**: "Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones".

- **Decreto 1080 de 2015**: "Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura". Este decreto recopila los decretos 2578 de 2012, 2609 de 2012, 1515 de 2013, 2758 de 2013, 1100 de 2014, 029 de 2015, 103 de 2015 y 106 de 2015."
- **NTC-ISO 15489-1:2016**. Gestión de Registros. Principios: Esta norma define algunos términos esenciales y los principios para la gestión de registros, como también establece generalidades de un sistema para su gestión. Empieza por agrupar las acciones de "creación, captura, protección, clasificación, control, almacenamiento, uso, migración o conversión, y disposición", dentro del concepto de gestión de registros como un todo, y establece de manera general como definir, asignar y comunicar políticas y responsabilidades para un sistema de gestión de registros electrónicos. La norma no establece una metodología específica para diseñar e implementar un SGDEA, pero ilustra los procesos necesarios para la creación, captura y gestión de registros los cuales deben estar soportados en controles también explícitos en la norma. La aparición de esta norma responde a la necesidad de tomar mejores decisiones con un enfoque en la gestión de evidencia autorizada, y que este a disposición de quienes la necesiten en cualquier momento.
- **Decreto 1499 de 2017** por el cual se establecen los lineamientos generales para la integración de la planeación y la gestión.
- **Decreto 1008 de 2018**: "Política de Gobierno Digital" y su respectivo "Manual de Gobierno de Digital".
- **Decreto No. 169 del 01 de septiembre de 2018** "Por medio del cual se adopta el Modelo Integrado de Planeación y Gestión - MIPG- en la Gobernación de Bolívar y se crean los Comités necesarios para su adecuado funcionamiento'' y se dictan otras disposiciones".
- **Decreto No. 489 del 19 de noviembre de 2018** "Por medio del cual se modifica parcialmente el Decreto 169 de 2018, "Por medio del cual se adopta el Modelo Integrado de Planeación y Gestión - MIPG- en la Gobernación de Bolívar y se crean los Comités necesarios para su adecuado funcionamiento'' y se dictan otras disposiciones.
- **Acuerdo No. 004 del 30 de abril de 2019**: "Por el cual se reglamenta el procedimiento para la elaboración, aprobación, evaluación y convalidación, implementación, publicación e inscripción en el Registro único de Series Documentales – RUSD de las Tablas de Retención Documental – TRD y Tablas de Valoración Documental – TVD".
- **Resolución 1075 del 30 de octubre de 2019**: "Por medio del cual se adopta las Tablas de Retención Documental de la Gobernación de Bolívar".
- **ISO 30301** Información y documentación. Sistemas de gestión para los documentos. Requisitos. Creación y control de los documentos durante el tiempo necesario.
- **ISO 18492** Conservación a largo plazo de la información basada en documentos.
- **ISO 15801** Imagen electrónica. Información almacenada electrónicamente. Recomendaciones sobre veracidad y fiabilidad.
- **ISO 16175** Información y documentación. Principios y requisitos funcionales para documentos en entornos de oficina electrónica. Parte 1: Generalidades y declaración de principios.

Adicionalmente se consultaron las Guías Técnicas elaboradas por el Archivo General de la Nación y el Ministerio de Tecnologías de la Información y las Comunicaciones:

- **Guía de Implementación de un Sistema de Gestión de Documentos Electrónicos de Archivo**: Realizada por el Archivo General de la Nación (AGN) donde se presenta la alineación y desarrollo de sistemas de gestión y un proyecto con visión integradora que involucre el trabajo articulado de archivistas e ingenieros, además de la participación de cada uno de los dueños y ejecutores de los procesos como productores de la información en sus diferentes niveles: estratégicos, misionales y de apoyo.
- **Guía No.3**: Cero Papel de la Administración Pública, donde se desarrolla información de cómo las entidades deben documentar e implementar políticas y procedimientos para el control de la creación, recepción, transmisión, mantenimiento y disposición de los documentos, protegiendo estos frente a cualquier adición, supresión, modificación, utilización u ocultación no autorizadas.
- **Guía No. 4**: Cero Papel en la Administración Pública: Expediente Electrónico. Establece las propiedades del expediente electrónico desde su producción, conformación y archivo.
- **Guía No. 5**: Digitalización de los Documentos. El proceso tecnológico que permite convertir un documento en soporte análogo, en uno o varios ficheros electrónicos que contienen la imagen codificada, fiel e íntegra del documento, con certificación tecnológica de integridad, disponibilidad, fiabilidad y autenticidad.
- **Guía No.6:** Se exponen algunos argumentos y otros requerimientos que nos permiten dilucidar que la planeación, análisis y diseño de un SGDEA parte de la necesidad de entender la organización y desarrollar componentes especializados integrados que definan un sistema que materialice los procedimientos, manuales y políticas de gestión documental.

1.6. Documentos Asociados

El modelo de requisitos como instrumento de la gestión Archivística, se relaciona con los siguientes documentos internos:

- Programa de Gestión Documental – PGD
- Plan Institucional de Archivos – PINAR
- Sistema Integrado de Conservación – SIC
- Las actividades relativas a la Planeación y el Análisis del SGDEA de la Gobernación de Bolívar, deben estar alineadas con los principios orientadores del MIPG y con la Política de Gobierno Digital, la Política de Seguridad Digital y las demás políticas del modelo de función pública.

2. MODELO DE REQUISITOS

2.1. Canales de Comunicación de la Gobernación de Bolívar

La **Gobernación de Bolívar**, utiliza diferentes canales de comunicación para recibir y enviar información en relación con los funcionarios, usuarios y ciudadanos en general que requieren los servicios ofrecidos por la entidad.

Dentro de los canales de comunicación a cargo de la entidad están los siguientes:

Medio	Escenario	Ubicación	Horario de atención
Presenciales	Puntos de atención al ciudadano	Carretera Cartagena-Turbaco Km. 3, Sector El Cortijo	Lunes a viernes de 7:00 a.m. a 3:000 p.m.
	Buzón de sugerencias	Carretera Cartagena-Turbaco Km. 3, Sector El Cortijo	Lunes a viernes de 7:00 a.m. a 3:000 p.m.
Números Telefónicos	Línea gratuita nacional	(57)-(5)-6517444	Lunes a viernes de 7:00 a.m. a 3:000 p.m.
	Línea fija local	6517444	
Virtuales	Sitio web	https://www.bolivar.gov.co	Permanente
	Facebook	https://www.facebook.com/GobDeBolivar/	Permanente
	Twitter	Bolívar Primero @GobDeBolivar	
	Correo	contactenos@bolivar.gov.co	
	Correo notificaciones judiciales	notificaciones@bolivar.gov.co	
	Formulario de radicación de peticiones, quejas reclamos o sugerencias	http://servicios.bolivar.gov.co/RadicacionExterna/Default.aspx	

Figura 1: Canales comunicación Gobernación de Bolívar

A través de estos canales se establece la clasificación de los documentos que ingresan, transfieren y salen de la **Gobernación de Bolívar** en diferentes niveles de responsabilidad, iniciando de lo general a lo particular; es decir, que los servidores de ventanilla reciban y clasifiquen un primer nivel con el conocimiento básico del área competente para gestionar las solicitudes (series y dependencias) y en un segundo nivel la dependencia encargada de dar respuesta para clasificarlo por subserie y tipo documental, realizando filtros de acuerdo a los tipos documentales que maneja cada dependencia y de esta manera obtener informes detallados de la información que maneja la **Gobernación de Bolívar**, por tipo documental, subserie y serie.

2.2. Esquema general del manejo de datos en el Sistema de Gestión Documental

la **Gobernación de Bolívar** actualmente tiene dentro de sus activos de información, diferentes aplicativos y/o sistemas de información o repositorios documentales utilizados por la Entidad, como el SharePoint Online (O365), Sigob, Saigtweb,

Tecnoexpedientes, Safe, VUR, Zafiro, bolivar.gov.co, Pasaporte, Antimalware, Webvisor, ArcGIS, Planner, AD, BDC, VPNs, Aplicaciones de Microsoft 365 para negocios, Tecnologías de almacenamiento en nube, NAS, entre otros.

Las aplicaciones que generen documentos electrónicos de archivo deben garantizar las condiciones de contenido estable de la información y control de acceso, así como las características de autenticidad, integridad, fiabilidad y disponibilidad permitiendo como mínimo las siguientes opciones:

- Interoperabilidad entre los sistemas actuales y el SGDEA
- Servicio de transferencia de Documentos Electrónicos de Archivo al SGDEA

El flujo de la información en la Entidad se da de acuerdo con el siguiente esquema de manejo de datos:

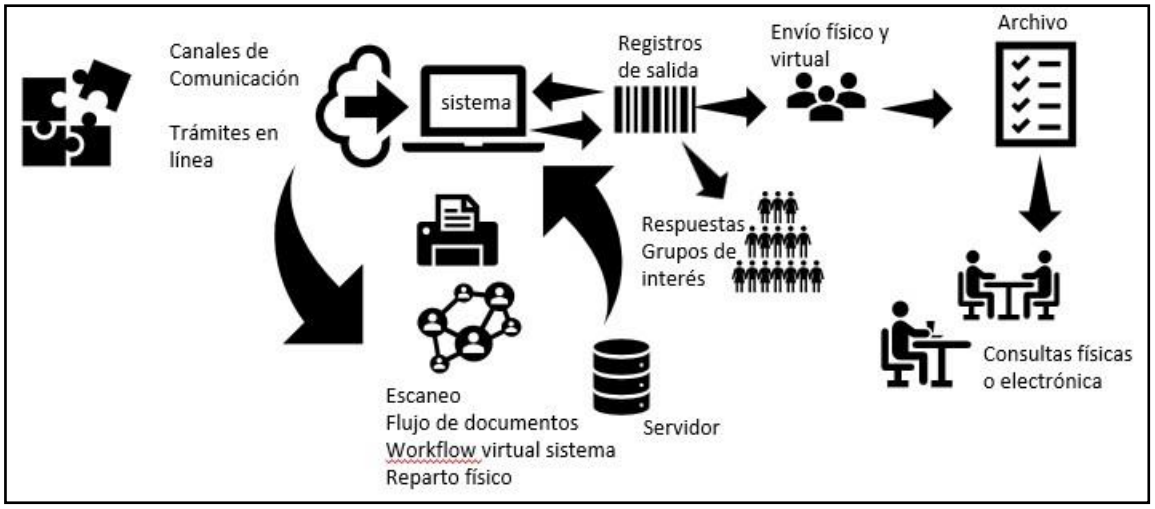

Figura 2: Esquema de manejo de datos e información Institucional

2.3. Sistema de Gestión de Documentos Electrónicos

El Sistema de Gestión de Documentos Electrónicos de Archivo de la **Gobernación de Bolívar** soportará una solución integral de la gestión documental con el apoyo de las tecnologías de la información. Ejemplo: Gestor documental que integre: Canales de comunicación, sistemas de información de la entidad, plataforma de gestión documental que permita el control documental en todas sus fases, administración integral de los actuales archivos, todo ello orientado a la implementación del documento electrónico de archivo para cumplir con la política Cero Papel, permitiendo reducir costos por administración de archivos y arrendamientos, personal, espacios, riesgos por perdida de documentos, tiempos, etc., dando una solución integral a la gestión documental de la entidad a largo plazo y sostenible.

2.3.1. Requisitos Funcionales.

2.3.1.1. Requisitos Funcionales de Configuración del SGDEA.

- La solución de gestión documental debe permitir realizar la captura, producción, tramite, administración, organización, almacenamiento, consulta, distribución, conservación y disposición final de contenido empresarial en la entidad.
- El sistema debe permitir gestión sobre el documento: creación, asignación, modificación, preparación, aprobación, reasignación, firma, respuesta y archivo.
- La solución debe incluir Funcionalidad para: Organizar, almacenar, proteger el contenido, administrar versiones, colaboratividad, flujos de trabajo, contenido social.
- La solución debe permitir la administración integral de la gestión archivística de la entidad (archivo de gestión, archivo central y archivo histórico), contenidos en documentos físicos y electrónicos, aplicando los lineamientos dados por el Archivo General de la Nación para la gestión archivística realizando como mínimo las actividades de creación de expedientes, clasificación de documentos, identificación de documentos, ordenación de documentos, descripción de documentos, ubicación de expedientes en estanterías, foliación, reconformación de expedientes, escaneo de folios, indexación de documentos, control de calidad, realizar préstamos y consultas de unidades archivísticas, realizar el control de las devoluciones de unidades archivísticas, rotulación, conservación, preservación y disposición final de acuerdo con las TRD y TVD.
- Debe permitir la administración y parametrización de la correspondencia con la que se pueden asignar o actualizar funciones a los usuarios sobre las radicaciones, las plantillas, firmas, tipos documentales, medio de envío y las que se requiera.
- Para tipos documentales debe permitir parametrizar dinámicamente por:

✓ Estado
✓ Días de retención
✓ Entrada
✓ Salida
✓ Control de términos por tramite (detener y activar).
✓ Finalizar términos

- Asociar al radicar un documento a una taxonomía específica y un trámite, contemplando:

✓ La clasificación (tipología) hasta de 5 niveles.
✓ Tipo documental de entrada y de salida.
✓ Flujo al que pertenece.
✓ Dependencia(s) asociadas con el flujo o trámite.
✓ Términos establecidos (días hábiles o calendario) para el trámite.
✓ Si está activo el trámite.
✓ Serie y subserie documental a la que pertenece.
✓ Si es un trámite de entrada y salida.
✓ Criterios de seguridad y permisos tiene: impresión, publicación, clasificación, etc.

- ✓ Disposición final del tipo documental o flujo: Ejemplo: eliminación, conservación, etc.
- La solución debe permitir la funcionalidad para la radicación de entrada y salida de correspondencia y las solicitudes recibidas, de todos los trámites de la Entidad, a través de diferentes medios, tales como: ventanilla y correo físico, ventanilla virtual, buzones y/o correos electrónicos, Redes sociales (mediante un link que direccione a los formularios para radicación de PQRS o con una leyenda escrita que dé a conocer que todos los tramites se deben realizar a través de la página institucional), Call Center,
  portal web y sitios web, fax server, CDs, USBs, etc.
- La solución debe permitir la firma mecánica (firma autógrafa) y digital de un documento, junto con su radicación con sus niveles de seguridad apropiados y la generación del archivo PDF/A para proteger el documento, registrando toda la operación para su trazabilidad.
- La solución debe permitir integrar la infraestructura necesaria para la digitalización de alta calidad y velocidad de cualquier fabricante, necesaria para la producción de una imagen digital a partir de un documento físico e integrar la digitalización de imágenes de excelente calidad con formato PDF/A y permitir la captura de texto y búsqueda por contenido OCR.

De igual forma, debe permitir:

- La asociación de imágenes a los documentos en todos los puntos de captura.
- Reconocimiento de formatos manuales preimpresos OMR, OCR, ICR.
- Procesamiento de formas electrónicas WEB, predefinidas para su diligenciamiento.
- Debe permitir la indexación para la creación de índices por atributos y/o metadatos, que permitan la identificación, clasificación y búsqueda de expedientes y documentos.
- Así mismo debe incluir la gestión de metadatos aprobada por la entidad, automatizando o autocompletando algunos datos para agilizar la captura. Para fortalecer la gestión documental de acuerdo con las TRD y la Clasificación del documento.
- Debe contener un gestor de documentos, contemplando los siguientes aspectos:
- ✓ Gestor de Imágenes.
- ✓ Gestor de Documentos Digitales o electrónicos.
- ✓ Gestor de registros.
- ✓ Gestor de Notificaciones de Actos Administrativos.
- ✓ Gestor de expedientes
- Integración con el Gestor Web o Sede Electrónica de la Entidad, lo que permitirá que todas los tramites de radicación se gestionen a través de la página institucional de la Gobernación de Bolívar. Para ello debe incluir los siguientes módulos:
- ✓ Administración de flujos de trabajo.
- ✓ Administración de tipos documentales.
- ✓ Administración de perfiles y permisos por flujo de trabajo.
- ✓ Administración de metadatos.

- ✓ Módulo de Archivo.
- ✓ Serie, subserie, tipologías documentales.
- ✓ Módulo de Calidad de la gestión documental.
- ✓ Módulo de Correspondencia y PQRSD.
- ✓ Módulo de notificaciones de actos administrativos.

- La solución debe permitir la importación y/o la definición dinámica, versionamiento y parametrización de las tablas de retención documental por periodos de tiempo e históricas, manteniendo la correlación entre ellas, por múltiples criterios, de acuerdo con las políticas y la normatividad existente.
- La solución ofrecida, debe permitir la gestión de documentos físicos e imágenes, sin perder la integridad lógica e indivisible, permitiendo el manejo y administración de grandes volúmenes de información, para su almacenamiento y recuperación, como también deben mantener estructura organizacional y las series, subseries y tipologías documentales, de acuerdo con las TDR o las TVD.
- La solución debe permitir definir y la parametrización de las tablas de valoración documental por periodos de tiempo e históricas, manteniendo la correlación entre ellas.
- La solución debe permitir el almacenamiento de archivos de imágenes en formatos comunes estándar como TIFF, MultiTIFF. JPEG y PDF, Video, Sonido, XML y cualquier otro formato de contenido.
- La solución debe permitir el escaneo de documentos individuales y por lotes en grandes volúmenes.
- La solución debe permitir sin desarrollo adicional la consulta de documentos y ejecución de flujos de trabajo desde dispositivos móviles incluidos iPad, iPhone, Android, etc.
- La solución debe proporcionar integración con clientes de correo electrónico de la entidad office 365, permitiendo a los usuarios acceso y funcionalidad de importación de correos electrónicos y documentos adjuntos en el repositorio, directamente desde su interfaz de correo electrónico.
- La solución debe incluir la funcionalidad que permita al procesador de importación de documentos procesar e importar automáticamente una secuencia de datos en XML y generar un informe cada vez que se ejecuta el proceso, indicando la finalización satisfactoria del proceso y los errores que se hayan producido.
- La solución debe incluir un módulo virtual para la gestión y administración de las peticiones, quejas, reclamos, sugerencias y denuncias; con capacidad para atender una alta demanda de solicitudes, indicando el estado en que se registra la solicitud y el número asignado.
- Este componente se debe integrar con toda funcionalidad de la solución ofrecida permitiendo su parametrización, gestión y trazabilidad de las solicitudes; generando las respectivas alarmas y reportes, de acuerdo con los niveles de servicio establecidos.
- Con el ingreso de la PQRSD por cualquiera de los diferentes canales (ventanilla física o virtual, página web, redes sociales, call center, correo electrónico, fax server, etc.) se deben ejecutar los flujos correspondientes al tipo de solicitud, queja o reclamo y sus respectivos controles de acuerdo con los tiempos de

respuesta y acuerdo de servicio; verificando la existencia del solicitante en el directorio o permitiendo su registro, para su notificación electrónica.

- La solución debe incluir un módulo de actos administrativos, dinámico y parametrizable; de carácter transversal, que permita la generación de este tipo de documentos desde los formatos establecidos, administración de versiones, la aprobación de los documentos con su respectiva numeración y firmas, hasta la comunicación y notificación de este.
- Debe controlar todos los eventos posteriores a la expedición y notificación de los actos administrativos, por ejemplo: la citación, notificación, avisos de publicación, recepción de recursos, ejecutorias, publicación de diario oficial, etc., el control de términos y las acciones posteriores.
- Debe proveer mecanismos de almacenamiento seguro y recuperación de los documentos generados a través de diversos criterios de búsqueda; así como también alarmas sobre los eventos, tiempos y reglas del negocio, que estén en riesgo de incumplimiento, sin perder la trazabilidad e interrelación con el respectivo expediente.
- La solución debe soportar múltiples tecnologías de almacenamiento en servidores, bases de datos, bodegas de datos y dispositivos de almacenamiento digital.
- La solución debe permitir la ubicación inmediata de todos los documentos que entran o que se generan a la Entidad, permitiendo y asignando el lugar de ubicación física en el archivo central y archivo general (Bodega, Estante, entrepaño, caja, carpeta, etc.).
- La solución debe permitir el cargue de los Inventarios Documentales utilizando el Formato Único de Inventario Documental Acuerdo 038 de 2002.
- La solución debe incluir Funcionalidad de gestión de registros: Políticas de retención de registros (documentos y dato estructurado), préstamos, seguimiento, auditoría, expedientes, estándares de calidad.
- La solución debe incluir Funcionalidad de gestión de imágenes: Escaneo, indexación, proceso automático de documentos, archivo digital.
- La solución debe permitir definir y parametrizar los grupos, roles y permisos de las dependencias y los usuarios de la Entidad que intervienen en el proceso documental, con los privilegios de acceso a los archivos y expedientes. Los cuales pueden ser totales, parciales por tipos documentales, entidad, etc., en concordancia con las TRD y tabla de control de acceso.
- La solución debe integra la clasificación de la información con fines de seguridad, de acuerdo con la normatividad vigente y las políticas de la Entidad, para la producción, gestión y almacenamiento de documentos físicos y digitales. Teniendo en cuenta las series, subseries, y otros criterios organizacionales.
- La solución debe integrar mecanismos que eviten la copia de documentos, en envío, la impresión, la edición, etc. a los documentos de acuerdo con su nivel de clasificación y confidencialidad, para evitar la fuga de información.
- Al detectar una acción de estas sobre cualquier documento debe generar la respectiva alarma y notificación a los administradores.
- La solución debe permitir la generación y uso de logs de auditoria con sus respectivos reportes.

- La solución debe proveer acceso remoto seguro para los funcionarios autorizados a través de la internet, mediante mecanismos de autenticación como certificados digitales o el registro de un dominio exclusivo para la entidad.
- La solución debe permitir la implementación de firmas digitales estandarizadas de cualquier proveedor autorizado en el País.
- La solución debe facilitar la administración de toda la documentación en todos los formatos. Garantizando su conservación de acuerdo con la Ley, que para algunos casos puede ser de mínimo 100 años, permitiendo su consulta y recuperación.
- La solución debe permitir controlar el préstamo de documentos de Archivo de Gestión, Archivo Central y Archivo histórico, identificando la trazabilidad de los documentos en préstamo y generando alertas para su devolución.
- La solución debe ser compatible con un número ilimitado de tipos y valores de metadatos por documento.
- La Solución debe permitir el manejo de diferentes formatos de metadatos.

2.3.1.2. Requisitos Funcionales de Creación e Ingreso de Documentos del SGDEA.

- La solución debe permitir la radicación física, debe ser ágil y amigable, permitiendo el ingreso de los datos básicos del documento, generando código QR e identificación de radicación. Debe contar como mínimo con la identificación del usuario, tipo de persona, entidad u organización, clasificación del tipo documental, digitalización, radicación, reparto, respuesta junto con la gestión y trazabilidad de acuerdo con los flujos establecidos.
- La solución debe permitir la impresión de rótulos de identificación o estampado en el fisco de label para original, copias y anexos, y que incluya con códigos de barras o QR para identificación del radicado.
- La solución debe permitir la recepción de documentos por diferentes medios: email, ventanilla, teléfono, fax, redes sociales, call center. Para estos últimos la recepción debe hacerse automáticamente.
- La solución debe la generación de rótulos o impresión de estampado del label debe ser automática en el momento de radicación y permitir la reimpresión por al administrador para casos especiales. Adicionalmente, deben permitir ser leído por un lector óptico permitiendo la identificación, ubicación física del documento (dependencia, archivo, estante, entrepaño, caja) y descripción de toda la información básica (metadato).
- El código de radicación debe contener como mínimo fecha, asunto, remitente, destinatario, cantidad de folios y los demás de acuerdo con las necesidades de la entidad (Metadatos) y de la normatividad vigente.
- Permitir la actualización de los metadatos asociados a una radicación, dejando el registro de auditoria y ejecutando automáticamente las reglas de negocio y los flujos de trabajo correspondientes.
- La solución debe permitir asociar 2 o más radicaciones asociadas a un mismo asunto, tema, servicio, proceso o trámite como función del funcionario de correspondencia o el caso contrario desasociar una radicación.

- La solución debe permite la vinculación o desvinculación de una radicación a uno o varios expedientes físicos y digitales, integrando el código QR como mecanismo de indexación respecto al expediente.
- La solución debe contener un directorio que permita incluir toda la información de un ciudadano, persona natural o jurídica, entidades de gobierno, con sus respectivos metadatos que permitan ser utilizados en las radicaciones de entrada y salida.
- Garantizar que una persona natural o jurídica, se pueda auto registrar en el portal web con sus datos; validando que no se puedan crear registros duplicados de esta información y permitir la búsqueda eficiente.
- La solución debe permitir el cruzar automáticamente el número único de radicado con el numero único de respuesta.
- La solución debe permitir la asignación de número único de radicación de entrada y salida.
- La solución debe incluir funcionalidades para radicación, indexación de mail, fax, casos y soportes desde telefonía (documentos físicos, electrónicos y voz).
- La solución debe permitir la gestión masiva de comunicaciones.
- La solución debe permitir y facilitar la digitalización de documentos físicos, para que fluyan digitalmente y no en físico, asociando los documentos digitalizados a los radicados, utilizando formatos estándar, eficientes y seguros.
- La solución debe permitir la identificación y clasificación de los documentos de acuerdo con lo definido por la Tabla de Retención Documental del Sistema de Gestión Documental de la Gobernación.
- La solución debe permitir el cálculo de la fecha de vencimiento del documento en días hábiles.
- La solución debe incluir mecanismos de verificación de documentos completos, que correspondan a lo anunciado, teniendo en cuenta los diferentes medios de envío y recibo (mensajería, físico, fax, correo electrónico, redes sociales, telefonía, etc.)
- La solución debe permitir diferentes niveles de caracterización de documentos y trámites por ejes temáticos.
- La solución debe permitir el manejo de comunicaciones urgentes o prioritarias, por ejemplo, tutelas.
- La solución debe permitir búsqueda de documentos y expedientes por diferentes criterios.
- La solución debe permitir la Generación de expedientes electrónico de archivo siguiendo los lineamientos del Archivo General de la Nación y su parametrización.
- La solución debe permitir facilidades para confrontar en cada área o dependencia el documento y el trámite para determinar claramente su competencia.
- La solución debe permitir la confirmación de recepción de correspondencia enviada a los usuarios, todo debe darse a través de la integración de dicha solución tecnológica con el sistema de gestión del correo institucional.
- La solución debe permitir la generación de reportes de gestión, en tiempo real.
- La solución debe permitir controlar las devoluciones de documentos, indicando las causas.

- La solución debe permitir la radicación de documentos internos cuyo destino sea interno o externo se debe realizar desde el área que los produce.

2.3.1.3. Requisitos Funcionales de Clasificación, Organización, Retención y Disposición Final en el SGDEA.

- El SGDEA debe permitir la creación, importación, parametrización, automatización, administración y versionamiento de las TRD, a partir de plantillas predefinidas, asistentes de configuración, cargue de archivos planos o a través de la incorporación de otros mecanismos que faciliten la administración y la gestión de las TRD.
- El SGDEA debe garantizar que los documentos producidos y asociados a una TRD, mantendrán los criterios de tiempos y de disposición final de la versión correspondiente.
- El SGDEA debe permitir modificar los tiempos de retención para un conjunto de series y/o expedientes.
- El SGDEA debe permitir que los documentos que componen el expediente hereden los tiempos de conservación establecidos en la TRD.
- El SGDEA debe garantizar que cualquier cambio a un tiempo de retención y disposición se aplique inmediatamente a todas las series, subseries a las que se asigna.
- El SGDEA debe incorporar múltiples niveles para el esquema del cuadro de clasificación documental
- El SGDEA debe validar la información que se ingresa en el esquema de la Tabla de Retención Documental a través de generación de alertas o incorporación de opciones que incluyan asistentes paso a paso (listas desplegables, alertas, listas de chequeo, ventanas de ayuda, entre otras) que indiquen si existe información similar o igual en el sistema.
- El SGDEA debe permitir a usuarios autorizados la selección y uso de las diferentes versiones de la TRD.
- El SGDEA debe permitir que el CCD y las TRD sean controladas únicamente por un rol administrador y que pueda agregar, modificar y reorganizar la estructura.
- El SGDEA debe permitir realizar la trazabilidad de los documentos electrónicos en el cuadro de clasificación documental mostrando información como mínimo de que, quien, cuando y como realizó acciones en el mismo.
- El SGDEA debe permitir la reubicación de una carpeta (o conjunto de carpetas) o documento, a un lugar distinto dentro de la estructura de clasificación, y garantizar que se mantengan los metadatos y demás atributos (permisos).
- El SGDEA debe permitir registrar las razones por las que se realiza la reubicación de cualquier elemento de la estructura de clasificación y almacenarlo como una propiedad o metadato.
- Una vez finalizado el trámite administrativo, el SGDEA debe incorporar opciones para el cierre del expediente. (manual o automático).
- Una vez cerrado el expediente se deberá restringir la adicción o supresión de carpetas o documentos.
- Excepciones: Cuando por disposiciones legales o administrativas sea necesario reabrir un expediente, esta acción deberá realizarse mediante un perfil

administrativo y debe quedar registro de ello en las pistas de auditoría, con la explicación del motivo por el cual se realizó la acción.

- El SGDEA debe permitir a un usuario autorizado aplazar la eliminación de una serie, subserie, expediente determinado. Cuando esto ocurra, el SGDEA debe solicitar y almacenar como mínimo la siguiente información en la pista de auditoría:

✓ La fecha de inicio de la interrupción.
✓ La identidad del usuario autorizado.
✓ El motivo de la acción.

- El SGDEA debe impedir la eliminación de un expediente electrónico o de su contenido. Sin embargo, existen dos excepciones a este requisito:

✓ La eliminación de acuerdo con lo establecido en las TRD.
✓ Eliminación por un rol administrativo como parte de un procedimiento auditado.

- El SGDEA debe permitir que todas las acciones efectuadas sobre el expediente deben ser registradas en un historial de eventos que puede ser consultado por usuarios que tengan acceso al expediente electrónico.
- El SGDEA debe permitir realizar la trazabilidad de los documentos electrónicos en el cuadro de clasificación documental mostrando información como mínimo de que, quien, cuando y como realizó acciones en el mismo.
- El SGDEA debe permitir que el historial de eventos del expediente electrónico pueda ser exportado. Igualmente, El SGDEA debe permitir exportar el directorio, de todos los expedientes y/o carpetas clasificadas en una serie específica y su contenido.
- El SGDEA debe permitir que las Tablas de Retención Documental tengan asociados los siguientes campos de manera opcional:

✓ Una descripción y/o justificación.
✓ Versión de la TRD.
✓ Fecha de actualización de la TRD en el sistema.
✓ Identificador único cuando se crea.

- El SGDEA debe permitir que la configuración del código de clasificación incluya: el formato del identificador asociado con cada nivel de la jerarquía, por ejemplo, numérico, alfabético; el primer valor de este identificador en cada clase, por ejemplo, 1, 1000, la presencia o ausencia de ceros iniciales; cualquier prefijo global.
- EL SGDEA debe admitir la creación de un esquema de clasificación, tablas de retención documental (TRD) o tablas de valoración documental (TVD), en el momento de la configuración para la captura y/o importación de documentos electrónicos.
- El SGDEA debe poder admitir un esquema de clasificación que pueda representar archivos y registros organizados en una jerarquía de clases. Igualmente, debe facilitar su modificación y el uso simultáneo de múltiples esquemas de clasificación de ser necesario. Esto podría ser requerido, por ejemplo, al seguir la fusión de dos organizaciones o la migración de sistemas anticuados. No está previsto para un uso rutinario.
- EL SGDEA debe permitir la gestión del o los esquemas de clasificación únicamente por un rol administrativo.

- El SGDEA debe proporcionar un mecanismo para asignar automáticamente un código de clasificación jerárquica a cada clase, archivo, sub-archivo y volumen en el esquema de clasificación.
- Cuando el SGDEA importa los metadatos de un esquema de clasificación, tablas de retención documental (TRD) o tablas de valoración documental (TVD), el SGDEA debe asignar a cada clase importada un código jerárquico de acuerdo con una opción establecida por un rol administrativo. Para esto, es importante definir reglas y procedimientos en un manual para la creación y configuración del o los esquemas de clasificación.
- Cuando el SGDEA importa los metadatos de un esquema de clasificación, debe rechazar cualquier clase que no tenga un título y crear un informe de excepción para un rol administrativo que enumere las clases que fueron rechazadas.
- El SGDEA debe permitir copiar, dividir, combinar o reubicar clases dentro del o los esquemas de clasificación.
- El SGDEA debe admitir la capacidad de crear múltiples entradas para un registro electrónico, en varias clases, archivos, sub-archivos o volúmenes electrónicos, sin duplicación del registro o del documento en el que se basa.
- El SGDEA debe permitir convenciones de nombres o tesauros que sean definidos en el momento en que se configura el sistema de gestión de documentos electrónicos. Cuando un vocabulario controlado de palabras clave toma la forma de un tesauro compatible con ISO 2788 o ISO 5964, el SGDEA debería poder imprimir las entradas del tesauro, mostrando todos los términos y sus relaciones.
- El SGDEA no debe permitir ninguna reubicación o copia que resulte en: almacenar cualquier sub-archivo(s) o volumen (s) en una clase del esquema de clasificación que se ha configurado para no permitir sub-archivos o volúmenes; almacenar cualquier registro (s) directamente en una clase que ya contenga cualquier archivo (s) o viceversa; almacenar cualquier archivo (s) en una clase que ya contiene alguna (s) clase (s) o viceversa.
- Debe ser posible que un Rol Administrativo configure el SGDEA en el momento de la configuración o más tarde para eliminar la capacidad de crear sub-archivos y / o volúmenes dentro de los archivos en todo el esquema de clasificación.
- Debe ser posible que un Rol Administrativo configure el SGDEA en el momento de la configuración o más adelante para permitir que solo se creen sub-archivos dentro de los archivos dentro de las clases especificadas del esquema de clasificación.
- Debe ser posible que un Rol Administrativo configure el SGDEA en el momento de la configuración o más adelante para permitir que solo se creen volúmenes dentro de los archivos dentro de las clases especificadas del esquema de clasificación.
- El SGDEA debe producir un informe que detalle cualquier falla durante la configuración del esquema de clasificación, la captura, transferencia, exportación, destrucción o eliminación. El informe debe identificar cualquier registro, agregación y metadatos asociados destinados a la transferencia que hayan generado errores de procesamiento, y cualquier entidad que no se haya transferido, exportado, destruido o eliminado con éxito.

- El SGDEA debería poder proporcionar soporte automatizado para decisiones sobre la clasificación de registros electrónicos para que: un subconjunto de un esquema de clasificación sea accesible para un usuario o rol; y/o identificar las clases o archivos utilizados más recientemente por ese usuario; y/o sugerir las clases o archivos utilizados con mayor frecuencia por ese usuario; y/o sugerir clases o archivos por inferencias extraídas de elementos de metadatos de registros (por ejemplo, palabras significativas utilizadas en el título o línea de asunto del correo electrónico); y/o sugerir clases o archivos por inferencias extraídas del contenido del registro.
- El SGDEA debería definir, en el cuadro de clasificación, agrupaciones no electrónicas y volúmenes, permitir la presencia de documentos no electrónicos en estos volúmenes que se reflejarán y manejarán del mismo modo que los documentos electrónicos.

2.3.1.4. Requisitos de Búsqueda, Recuperación y Reproducción.

- El SGDEA debe Proporcionar un rango flexible de funciones que operen con los metadatos relacionados con cada nivel de la agrupación y en los contenidos de los documentos a través de los parámetros definidos para el usuario con el propósito de ubicar, acceder y recuperar documentos individuales o grupos de documentos o metadatos.
- El SGDEA debe permitir que todo documento, volumen o metadatos de la gestión de documentos de la agrupación puedan ser buscados.
- El SGDEA debe permitir al usuario buscar y recuperar información que se encuentre dentro de documentos, listas de documentos y metadatos, de acuerdo con el perfil de acceso.
- El SGDEA debe proporcionar una función de búsqueda que permita utilizar combinaciones de criterios de búsqueda:

✓ Operadores booleanos (y, o, exclusivo, o, no).
✓ Coincidencias aproximadas.
✓ Intervalos de tiempo.
✓ Permitir búsqueda con comodines (*,? , $, = , + , -).
✓ Por agrupaciones (Código, Serie, subseries, asunto, usuario, área responsable, palabras clave...).
✓ Tipos de formatos.
✓ Cualquier combinación valida con un número limitado de criterios de búsqueda, utilizando cualquier combinación de contenido textual o de metadatos.
✓ Opción de autocompletar.

- El SGDEA debe permitir:

✓ Ver la lista de resultados de una búsqueda.
✓ Listar documentos que componen un resultado de la búsqueda.
✓ Ver la lista de todos los expedientes y documentos relacionados a cualquier serie determinada, con su respectivo contenido.
✓ Incluir funciones para presentar en los medios adecuados la salida de los documentos que no se pueden imprimir. Por ejemplo, documentos de audio y video.

- ✓ Mostrar miniaturas de imágenes digitalizadas como una ayuda para la navegación y búsqueda.
- El SGDEA debe permitir que los administradores configuren y cambien los campos de búsqueda para:
- ✓ Especificar cualquier elemento del documento, volumen y de la agrupación de los metadatos de la gestión de documentos, y opcionalmente todo el contenido del documento, como campos de Búsqueda.
- ✓ Cambiar la configuración del campo de búsqueda.
- El SGDEA debe permitir visualizar los documentos de archivo recuperados como resultado de la búsqueda sin necesidad de cargar la aplicación de software asociada.
- El SGDEA debe permitir que en los resultados de búsqueda se presenten únicamente las carpetas y documentos a los que el usuario tiene acceso de acuerdo con los niveles de permisos definidos.
- El SGDEA debe permitir la búsqueda dentro de una única agrupación o a través de más de una agrupación.
- El SGDEA debe ofrecer una clasificación de los resultados de la búsqueda, según su pertinencia, relevancia, fechas, nombre, autor, creador, modificador, tipo de documento, tamaño, entre otros.
- El SGDEA debe permitir que ninguna función de búsqueda revele jamás al usuario información como contenido o metadatos, que se le tengan restringidos por permisos de acceso.
- El SGDEA debe permitir la previsualización de documentos del expediente, sin que eso implique la descarga del documento.
- El SGDEA debe ser capaz de buscar, recuperar y mostrar todos los documentos y metadatos de la gestión de documentos relacionados con una agrupación electrónica, o volumen, como una unidad única.
- El SGDEA debe ser capaz de buscar, recuperar y reproducir una agrupación electrónica a través de todos los principios de nomenclatura implementados, incluyendo:
- ✓ Nombre.
- ✓ Identificador (código de clasificación).
- El SGDEA debe poder mostrar el número total de resultados de búsqueda en la pantalla del usuario y se deberá permitir que luego el usuario muestre la lista de resultados, o perfeccione los criterios de búsqueda y realice otra solicitud.
- EL SGDEA debe permitir que los documentos y agrupaciones que aparecen en la lista de resultados de la búsqueda puedan ser seleccionados y luego abiertos (de acuerdo con los controles de acceso) con un simple clic o tecleado.
- El SGDEA debe permitir que los usuarios recuperen agrupaciones y documentos directamente a través del uso de un identificador único.
- El SGDEA no puede permitir nunca que una búsqueda o que la recuperación revele a un usuario cualquier información (metadatos de la gestión de documentos o contenido del documento) que los ajustes de seguridad y acceso pretendan esconder de dicho usuario.

- El SGDEA debe integrar facilidades de búsqueda para todos los niveles del cuadro de clasificación. Es decir, los usuarios deberían utilizar la misma interfaz, características y opciones cuando busquen clases, agrupaciones o documentos.
- El SGDEA debe realizar búsquedas a través de las agrupaciones híbridas no electrónicas y electrónicas, y Permitir a los usuarios perfeccionar (estrechar) las búsquedas. Por ejemplo, un usuario debería ser capaz de comenzar con la lista de resultados de una búsqueda y luego iniciar una búsqueda dentro de la lista.
- El SGDEA debe incluir características para reproducir estos documentos que no pueden ser impresos a través de un dispositivo de salida. Los ejemplos incluyen audio, video y algunos sitios web.

2.3.1.5. Requisitos Funcionales de Acceso, Seguridad, Controles de Acceso, Controles de Seguridad y Niveles de Seguridad del SGDEA.

- El SGDEA debe permitir establecer niveles de seguridad del expediente de acuerdo con los niveles de seguridad establecidos por la entidad.
- El SGDEA debe permitir la creación y administración de usuarios, roles y permisos.
- El SGDEA debe permitir revocar privilegios de un grupo o usuarios seleccionados.
- El SGDEA debe ofrecer opciones de configuración para asignar o eliminar roles después de un período predefinido automáticamente.
- El SGDEA debe permitir configurar controles restringir el acceso de acuerdo con los perfiles configurados por el administrador del sistema.
- El SGDEA se debe permitir siempre la generación y aplicación del método de autenticación de doble factor.
- El SGDEA debe asegurar que los documentos se mantienen completos e inalterados, excepto en determinadas circunstancias como órdenes judiciales de enmiendas para grabar el contenido y los metadatos, en qué casos sólo los administradores del sistema pueden emprender tales cambios con la autorización apropiada.
- El SGDEA debe permitir múltiples firmas electrónicas o digitales en los documentos electrónicos.
- El SGDEA debe permitir parametrizar firmas individuales, múltiples firmantes, firmas masivas de documentos y firmas por lotes de documentos.
- El SGDEA debe permitir la integración con mecanismos tecnológicos tales como: firmas digitales, estampado cronológico, mecanismos de encriptación y marcas digitales electrónicas
- EL SGDEA debe permitir la creación, gestión y configuración de niveles de clasificación de información a que haya lugar (Clasificada, reservada, confidencial, de acuerdo con la normatividad existente) y permitir acceso a esta dependiendo el rol de usuario.
- El SGDEA no debe limitar el número de roles o grupos que se puedan configurar.
- El SGDEA debe permitir configurar y ejercer controles sobre tiempos de inactividad y bloqueo.
- Mantener la integridad técnica, estructural y relacional de los documentos y metadatos en el sistema.

- Permitir que el administrador limite el acceso a los documentos, agrupaciones y metadatos de la gestión de documentos a usuarios específicos o grupos de usuarios.
- El SGDEA debe Permitir que el administrador altere la categoría de seguridad de los documentos individuales. Esto es requerido de manera rutinaria para reducir el nivel de protección dado a los documentos ya que su receptividad disminuye con el tiempo.
- EL SGDEA debe permitir cambios en los atributos de seguridad para grupos o usuarios (como derechos de acceso, nivel de seguridad, privilegios, asignación de la contraseña inicial y de gestión) que sólo puedan ser realizados por el administrador.
- El SGDEA debe permitir que sólo el administrador adjunte los atributos del perfil del usuario que determine las características, campos de los metadatos de la gestión de documentos, documentos o agrupaciones a los que el usuario tiene acceso. Los atributos del perfil: prohibirán el acceso al sistema de gestión de documentos sin un mecanismo de autenticación aceptado atribuido al perfil del usuario; restringirá el acceso del usuario a documentos específicos o agrupaciones; restringirá el acceso del usuario de acuerdo a la autorización de seguridad del usuario; restringirá el acceso del usuario a determinadas características (por ejemplo, lectura, actualización y/o borrar determinados campos de los metadatos de gestión de documentos); denegará el acceso luego de una fecha específica; asignará el usuario a un grupo o grupos.
- El SGDEA debe ser capaz de proporcionar las mismas funciones de control para roles, y para usuarios. Esta característica permite al administrador gestionar y mantener un conjunto limitado de roles con derecho de acceso más que amplio número de usuarios individuales. Ejemplo de roles pueden incluir al Gerente, Oficina de Quejas, Analista de Seguridad o Administrador de la Base de Datos.
- El SGDEA debe ser capaz de establecer grupos de usuarios que están asociados con una agrupación, y permitir que un usuario sea miembro de más de un grupo.
- El SGDEA debe permitir que un usuario estipule que otros usuarios o grupos puedan acceder a los documentos de los que el usuario es responsable, siempre y cuando el rol administrativo lo autorice.
- El SGDEA no debe permitir que ninguna persona lleve a cabo ninguna acción en el SGDEA, a menos que, la persona sea un usuario autorizado que haya sido identificado y autenticado con éxito.
- El SGDEA debe permitir que los roles administrativos agreguen y eliminen usuarios desde y hacia los roles y grupos en cualquier momento.
- El SGDEA debe permitir la integración con el directorio activo corporativo.
- El SGDEA debe permitir que las contraseñas nunca pueden ser almacenadas en formato texto. Deben ser almacenadas por medio de un algoritmo de encriptación de una sola vía reconocido por la industria como es el mecanismo SHA2. Para estos procesos de cifrado se deben utilizar llaves cuya longitud mínima debe ser de 256 palabras.
- EL SGDEA debe aplicar técnicas criptográficas en las operaciones y/o transacciones críticas o sensibles para la Organización.

- El SGDEA debe desconectar los usuarios que hayan permanecido inactivos en el sistema durante un tiempo definido mediante un parámetro que especifique este tiempo.
- El SGDEA debe permitir marcar un usuario individual como inactivo, sin eliminarlo del sistema.
- El SGDEA debe permitir definir por parámetro y controlar la vigencia mínima, vigencia máxima y tiempo de aviso de vencimiento, de las contraseñas.
- El SGDEA debe permitir manejar los siguientes estados para las cuentas de usuario: Habilitado, deshabilitado, bloqueado, suspendido.
- El SGDEA debe permitir rastrear de forma automática y sin ninguna intervención manual todas las acciones realizadas en el sistema, y almacenar los datos sobre estas en la pista de auditoría.

2.3.1.6. Requisitos Funcionales de Ejecución de Controles de Seguridad y Categorías de Seguridad del SGDEA.

- El sistema de gestión de documentos electrónicos debe permitir alterar la categoría de seguridad de todos los documentos, dentro de una agrupación, en una sola operación. Igualmente, debe proporcionar una advertencia si las clasificaciones de seguridad de cualquier documento son alteradas, y esperar la confirmación antes de completar la operación.
- EL SGDEA debe grabar todos los detalles de cualquier cambio de la categoría seguridad en los metadatos de la gestión de documentos, volumen o agrupación afectada.
- El SGDEA debe poder capturar y almacenar, cuando corresponda, cualquier intento de violación de los mecanismos de control de acceso (es decir, los intentos de un usuario de acceder a un registro, volumen, sub-archivo o archivo al que se le deniega el acceso).
- Registrar todos los intentos no autorizados para acceder a las agrupaciones (y sus volúmenes) o documentos en sus respectivos y únicos metadatos.
- El SGDEA debe permitir la generación de registros de control o hashes que permitan validar la integridad de los registros de seguridad generados.
- El SGDEA debe generar y mantener pistas de auditoría inalterables de las acciones realizadas por cada uno de los usuarios que ingresan al sistema.
- El SGDEA debe capturar y almacenar en las pistas de auditoría, como mínimo información sobre:

✓ Toda acción realizada sobre cada documento, expediente, usuario y metadatos.
✓ Toda acción realizada en los parámetros de administración.
✓ Usuario que realiza la acción.
✓ Fecha y hora de la acción.
✓ Cambios realizados a los metadatos.
✓ Cambios realizados a los permisos de acceso.
✓ Creación, modificación o eliminación de usuarios, grupos o roles del sistema.
✓ País, navegador, dirección IP, tipo de dispositivo, sistema operativo, desde donde fue abierta la sesión del sistema.

- El SGDEA debe mantener las pistas de auditoría en el sistema durante el tiempo que se haya establecido en las políticas de la Entidad y las normas aplicables.
- El sistema debe impedir desactivar la generación y almacenamiento de las pistas de auditoría.
- Las pistas de auditoría del SGDEA deben permitir identificar los errores en la ejecución de los procesos. (Mantenimiento en menor tiempo).
- El SGDEA debe permitir a un usuario autorizado parametrizar el número de intentos fallidos de ingreso a la sesión.
- El SGDEA deberá bloquear al usuario una vez se hayan completado el número de intentos fallidos configurados por el usuario autorizado para el inicio de sesión y notificar mediante un mensaje de alerta.
- El SGDEA debe permitir generar informes con los datos almacenados en las pistas de auditoría, permitiendo filtros y selección de criterios establecidos por el usuario solicitante.
- El SGDEA debe permitir programar rutinas de copia de seguridad (backups) y su recuperación cuando sea necesario.
- El SGDEA debe permitir la parametrización de copias de seguridad de los documentos en conjunto con los metadatos.
- El SGDEA debe notificar al usuario encargado, fallas críticas en los servicios del sistema en el instante en que se presentan.
- EL SGDEA debe garantizar que las operaciones realizadas en el sistema deben estar protegidas contra adulteración, supresión, ocultamiento y demás operaciones que atenten contra la autenticidad, integridad y disponibilidad de la información.
- EL SGDEA debe contar con mecanismos de recuperación de credenciales de acceso obedeciendo las políticas de ingreso seguro.
- El SGDEA debe prevenir la destrucción o supresión de cualquier documento por cualquier usuario, incluyendo un administrador con las excepciones de: destrucción de acuerdo con lo dispuesto por la autoridad.
- El SGDEA debe ser capaz de determinar la más alta categoría de seguridad de cualquier documento en cualquier agrupación por medio de una simple pregunta.
- El SGDEA debe restringir el acceso a agrupaciones electrónicas/documentos que tengan una clasificación de seguridad más elevada que el espacio de seguridad del usuario.
- El SGDEA Ser capaz de prevenir una agrupación electrónica de tener una clasificación de seguridad baja respecto de cualquier documento electrónico dentro de la agrupación.
- El SGDEA debe permitir que las clasificaciones de seguridad sean asignadas a los documentos. La clasificación de seguridad será asignada jurídica u organizacionalmente, pero debe incluir niveles de categoría tales como:

✓ Sin clasificar.
✓ En confidencia (política y privacidad).
✓ Delicado (política y privacidad).
✓ Restringido (información sobre seguridad nacional).
✓ Confidencial (información sobre seguridad nacional).
✓ Secreto (información sobre seguridad nacional).
✓ Muy secreto (información sobre seguridad nacional).

- Se deberá tener mayor cautela para cualquier nivel de autorización de seguridad.
- Permitir que las clasificaciones de seguridad sean seleccionadas y asignadas a nivel del sistema para: todos los niveles de agrupaciones de documentos (incluyendo volúmenes); documentos individuales u objetos de los documentos.

2.3.1.7. Requisitos Funcionales de Gestión de Metadatos del SGDEA.

- El SGDEA debe capturar y almacenar en las pistas de auditoría, como mínimo información sobre:
  - ✓ Toda acción realizada sobre cada documento, expediente, usuario y metadatos.
  - ✓ Toda acción realizada en los parámetros de administración.
  - ✓ Usuario que realiza la acción.
  - ✓ Fecha y hora de la acción.
  - ✓ Cambios realizados a los metadatos.
  - ✓ Cambios realizados a los permisos de acceso.
  - ✓ Creación, modificación o eliminación de usuarios, grupos o roles del sistema.
  - ✓ País, navegador, dirección IP, tipo de dispositivo, sistema operativo, desde donde fue abierta la sesión del sistema.
- El SGDEA debe ser capaz de crear metadatos inalterables de las acciones de gestión de documentos (acciones que deberán ser especificadas por la organización) que se toman sobre los documentos, agrupaciones o el cuadro de clasificación. Los metadatos deberían incluir los siguientes elementos de los metadatos de la gestión de documentos:
  - ✓ Tipo de acción de la gestión de documentos.
  - ✓ Usuario que inicie y/o lleve a cabo la acción.
  - ✓ Fecha y tiempo de la acción.
- El SGDEA debe permitir diligenciar metadatos de ubicación, que luego van a permitir su ubicación a nivel de unidades documentales, para el caso de los expedientes híbridos.
- El SGDEA debe permitir la búsqueda de texto libre y metadatos de forma integrada y coherente.
- Durante un proceso de migración entre diferentes sistemas o plataformas tecnológicas se debe garantizar que:
  - ✓ Exportar o transferir los documentos correspondientes con las reglas de retención y disposición y sus respectivos controles de acceso (seguridad para consulta) para que puedan seguir aplicándose en el sistema de destino.
  - ✓ Exportar uno o más informes o reportes que muestren las reglas que se aplicarán a cada conjunto de documentos con sus características.
  - ✓ Garantizar la estructura del expediente garantizando que los vínculos archivísticos se conserven en todo momento.
- El SGDEA debe poder mantener los metadatos tanto tiempo como se requiera.
- El SGDEA debe permitir generar informes con los datos almacenados en las pistas de auditoría, permitiendo filtros y selección de criterios establecidos por el usuario solicitante.

- El SGDEA debe permitir registrar las razones por las que se realiza la reubicación de cualquier elemento de la estructura de clasificación y almacenarlo como una propiedad o metadato.
- El SGDEA debe ser capaz de exportar metadatos para documentos específicos y grupos selectos de documentos sin afectar los metadatos almacenados por el sistema de gestión de documentos electrónicos. Esta funcionalidad puede ser utilizada por auditores externos que deseen examinar o analizar la actividad del sistema.
- EL SGDEA debe poder asegurarse de que los metadatos están disponibles para ser inspeccionados según pedido, de modo que un evento específico puede ser identificado y todos los datos relacionados puedan estar disponibles, y que ello pueda ser conseguido por personal externo autorizado que no tenga familiaridad o muy poca con el sistema.
- El SGDEA debe proporcionar metadatos de todos los cambios hechos a:

✓ Agrupaciones electrónicas (incluyendo volúmenes); ✓ documentos electrónicos individuales.

✓ Metadatos de gestión de documentos asociados con cualquiera de los elementos mencionados arriba.

- El SGDEA debe realizar seguimiento de auditoría de todos los cambios a los valores de metadatos que se aplican a los elementos de metadatos.
- Permitir que el conjunto de elementos de metadatos de la gestión de diferentes documentos sea configurado para agrupaciones electrónicas y no electrónicas; los metadatos de la gestión de documentos de la agrupación deberán incluir información sobre la ubicación física de la agrupación no electrónica.

2.3.1.8. Requisitos Funcionales de Flujos de Trabajo del SGDEA.

- El SGDEA debe permitir la creación, administración y ejecución de flujos.
- El SGDEA debe permitir diagramar y modelar flujos electrónicos.
- El SGDEA debe permitir diagramar tareas que componen un proceso y/o procedimiento.
- El SGDEA debe permitir parametrizar los tiempos de ejecución y respuesta de los procesos ejecutados.
- El SGDEA debe permitir incorporar un mecanismo de simulación para analizar los flujos de trabajo modelados.
- El SGDEA debe permitir la administración y control de los procesos por lotes y los procesos automáticos programados.
- El SGDEA debe permitir parametrizar los accesos, creación, modificación o control total para usuarios o grupos de usuarios de los flujos de trabajo.
- El SGDEA no debe limitar el ingreso de acciones que componen cada flujo de trabajo.
- El SGEDEA debe permitir contener múltiples versiones de un mismo proceso y/o procedimiento. Debe permitir al administrador seleccionar la última versión.
- El SGDEA debe generar una trazabilidad de las acciones de los flujos de trabajo e incluirla en las pistas de auditoría.
- El SGDEA debe permite definir los flujos de trabajo basado en plantillas.

- El SGDEA debe permitir detener un flujo de trabajo.
- Definir los tiempos límite de ejecución de los flujos y de cada una de sus actividades enviando notificaciones de incumplimiento.
- Contar con semáforos que muestran el cumplimiento de tiempos en cada una de las actividades de un flujo.
- Cuando el período de retención aplicable a algunos registros debido a un programa de retención y disposición llega a su fin, el SGDEA debe iniciar automáticamente el procesamiento de la decisión de disposición.
- Cuando se ejecuten las autoridades de disposición, el sistema de gestión de documentos electrónicos debe ser capaz de:

✓ Confeccionar un informe de excepción para el administrador.
✓ Eliminar todos los contenidos de una agrupación o volumen cuando sean borrados.
✓ Invitar al administrador a que ingrese una razón para la acción.
✓ Asegurar que no se borren ítems si su eliminación implica un cambio en otro documento (por ejemplo, si un documento forma parte de dos documentos - ver Sección: Agrupación de documentos electrónicos - uno de los cuales está siendo eliminado).
✓ Informar al administrador de cualquier vínculo de una agrupación o documento con otra agrupación o volumen, que está por ser eliminado, y pedir la confirmación antes de completar la eliminación.
✓ Alertar a los administradores de cualquier conflicto, por ejemplo, ítems que están vinculados con más de una acción de disposición que involucra indicadores.
✓ Mantener completa la integridad de los metadatos de la gestión de documentos en todo momento.

- El SGDEA debe permitir que el administrador, manual o automáticamente, cierre o bloquee los procesos de disposición de los documentos (bloquear para propósitos de investigación legal, propósitos de libertad de información, etc.).
- El SGDEA debe almacenar en los metadatos todas las decisiones tomadas por el revisor durante las revisiones.
- El SGDEA debe realizar un informe de parte de la autoridad de disposición al administrador que identifique a todas las autoridades de disposición que deben actuar en un período determinado de tiempo, y proporcionar informes cuantitativos sobre la cantidad y tipo de documentos cubiertos.
- El SGDEA debe alertar al administrador sobre si una agrupación electrónica que debe ser destruida, está referida a un vínculo de otra agrupación y pausar el proceso de destrucción para permitir que la siguiente acción a ser tomada remedie:

✓ Confirmación del administrador para proceder con o cancelar el proceso;
✓ Generar un informe detallando la agrupación o documentos concernientes y todas las referencias o vínculos para los que está destinado.

- El SGDEA debe proporcionar o apoyar la capacidad de interactuar con la facilidad de flujo de trabajo para apoyar la programación, revisión y el proceso de exportación/transferencia por rastreo.
- El SGDEA debe apoyar la elaboración de informes y las herramientas de análisis para la gestión de retención y las autoridades de disposición por parte del administrador, incluyendo la habilidad de:

- ✓ Listar todas las autoridades de disposición.
- ✓ Listar todas las agrupaciones electrónicas a las que se les asigna una autoridad de disposición específica.
- ✓ Listar la(s) autoridad(es) de disposición que se aplican a todas las agrupaciones por debajo de un punto especificado en la jerarquía del cuadro de clasificación.
- ✓ Identificar, comparar y revisar las autoridades de disposición (incluyendo sus contenidos) a través del cuadro de clasificación.
- ✓ Identificar las contradicciones formales en las autoridades de disposición a través del cuadro de clasificación.
- El SGDEA debe permitir que el administrador ingrese comentario en los metadatos de la gestión de documentos de la agrupación para registrar las razones de las decisiones de la revisión.
- El SGDEA debe almacenar en los metadatos todas las decisiones tomadas por el revisor durante las revisiones.

2.3.2. Requisitos No Funcionales.

- El SGDEA debe proporcionar ayuda en línea en todo el sistema.
- Todos los mensajes de error producidos por el SGDEA deben ser significativos y coherentes, para que los usuarios puedan decidir cómo corregir el error o cancelar el proceso. Idealmente, cada mensaje de error irá acompañado de un texto explicativo y una indicación de las acciones que el usuario puede realizar en respuesta al error.
- La interfaz de usuario de SGDEA debe ser adecuada para usuarios con la gama más amplia de necesidades y capacidades; es decir, diseñado de acuerdo con las normas de accesibilidad adecuadas, y compatible con el software de accesibilidad especializado común.
- El SGDEA debe ser fácil de usar e intuitivo en todo momento para cualquier persona.
- El SGDEA debe ser escalable y no permitir ninguna característica que impida su uso en organización de pequeño o gran tamaño, permitiendo aumentar la Capacidad del sistema para ofrecer más servicios a un mayor número de usuarios sin degradar la calidad del servicio.
- El SGDEA debe ser 100% web y su administración y parametrización debe realizarse desde el navegador. Se deben proveer interfaces de escritorio opcionales.
- El SGDEA debe estar estrechamente integrado con el sistema de correo electrónico de la organización para permitir que los usuarios envíen registros y agregaciones electrónicamente sin salir del SGDEA. Igualmente, debe proporcionar esto mediante el envío de punteros o enlaces a agregaciones y registros en lugar de copias, siempre que se envíe una agregación o registro a otro usuario de dicho sistema.
- El SGDEA debe permitir que los usuarios muevan, redimensionen y modifiquen la apariencia de las ventanas, y guarden las modificaciones en su perfil de usuario para que surtan efecto automáticamente cada vez que los usuarios inician sesión en el SGDEA.

- El SGDEA debe permitir a los usuarios personalizar aspectos de la interfaz gráfica de usuario. La personalización debe incluir, pero no debe limitarse a, los siguientes cambios: contenido del menú y de la barra de herramientas; diseño de la pantalla; uso de las teclas de función; colores en pantalla, fuentes y tamaños de fuente; alertas audibles. El SGDEA debe permitir menús desplegables configurables o "listas de selección" de valores de elementos de metadatos para la entrada de datos. El contenido de estas listas debe ser configurable por un rol administrativo.
- El SGDEA debe indicar si un mensaje de correo electrónico tiene un archivo adjunto. Por ejemplo, mediante un icono.
- El SGDEA debe permitir a los usuarios definir referencias cruzadas entre registros relacionados, tanto dentro de la misma agregación como en diferentes agregaciones, lo que permite una fácil navegación entre los registros.
- El SGDEA debe permitir que un usuario que tiene acceso a un archivo o registro verifique si otro usuario, grupo o rol especificado tiene acceso a él.
- EL SGDEA debe permitir a través de un rol administrativo un bloque temporal que prohíba el acceso a un determinado archivo o registro. Esta decisión debe justificarse y quedar muy bien documentada.
- El SGDEA debe permitir a los usuarios definir clases, archivos y registros como "favoritos", para que puedan encontrarlos fácilmente en ocasiones posteriores.
- El SGDEA debe contar con manuales de usuario estructurados adecuadamente.
- El SGDEA debe contar con un módulo de ayuda en línea.
- Toda funcionalidad del sistema y transacción de negocio realizada en el SGDEA debe responder al usuario en el menor tiempo posible.
- El SGDEA debe proporcionar tiempos de respuesta adecuados para satisfacer las necesidades comerciales de las funciones que se realizan comúnmente en condiciones estándar, por ejemplo: <100%> del total de usuarios anticipados registrados y activos.
- El SGDEA debe poder devolver los resultados de una búsqueda simple (la lista de resultados) dentro de <3 segundos> y de una búsqueda compleja (combinando cuatro términos) dentro de <10 segundos> independientemente de la capacidad de almacenamiento o el número de archivos y registros en el sistema. En este contexto, realizar una búsqueda significa devolver una lista de resultados. No incluye la recuperación de los registros en sí.
- El SGDEA debe permitir que una sola implementación del sistema tenga un almacén de registros electrónicos de al menos <xx gigabytes / terabytes / peta bytes> o <xx mil / millones / billones> de registros, y que sirva al menos <xx cien / miles> usuarios simultáneamente con los niveles de rendimiento especificados en esta sección; (estas necesidades técnicas saldrán y establecerán mediante la consultoría que se contrate para definir, las capacidades y la robusta del sistema que se espera y que esté acorde con las necesidades de la gestión institucional).
- Las estimaciones de los requisitos de almacenamiento y el registro y la población de usuarios deben ser insertados por la organización. Tenga en cuenta que, en grandes organizaciones, se pueden acumular grandes volúmenes de registros; en algunos casos esto se extenderá a los miles de millones de registros.
- El SGDEA debe ofrecer soporte para sistemas de almacenamiento tipo NAS, DAS y SAN (que en su momento es los estudios de necesidades técnicas se

determinara si estos equipos serán provistos por la Gobernación o el tercero que se pretenda contratar). Por lo que es necesario evaluar requisitos de rendimiento de las maquinas (servidores).

- Debe ser posible expandir el SGDEA, de manera controlada, para cumplir con el crecimiento organizativo hasta por lo menos <900.000 / mil> usuarios mientras se brinda continuidad de servicio.
- El SGDEA deberá estar disponible las 24 horas del día, 7 días de la semana, 365 días del año.
- El tiempo de inactividad no prevista del SGDEA, no debe superar las 10 horas al trimestre y 40 horas al año.
- La definición de "tiempo de inactividad" puede depender de la infraestructura y la arquitectura. Por ejemplo, en algunos entornos, una falla causada por el hardware del servidor se considerará como una falla del SGDEA.
- El SGDEA debe cumplir con las normas locales aplicables para la admisibilidad legal y el peso probatorio de los registros electrónicos.
- El SGDEA debe cumplir con lo expuesto en el decreto 2609 de 2012 y otras normas técnicas y legales vigentes.
- El SGDEA no debe incluir ninguna característica que sea incompatible con la protección de datos, la libertad de información u otra legislación técnica legal vigente.

2.3.3. Requerimientos Complementarios.

2.3.3.1. Management of Physical (Non-electronic) files and Records, and Disposition of Physical Records - Administración física de registros, documentos y disposición final de los mismos (conservación).

- El SGDEA debe permitir que ambos tipos de documento sean gestionados de manera integrada.
- El SGDEA debe permitir que una agrupación no electrónica que está asociada como híbrida con una agrupación electrónica, utilice el mismo título y código de referencia numérica, pero con la indicación de que se trata de una agrupación no electrónica híbrida.
- El SGDEA debe permitir que el conjunto de elementos de metadatos de la gestión de diferentes documentos sea configurado para agrupaciones electrónicas y no electrónicas; los metadatos de la gestión de documentos de la agrupación deberán incluir información sobre la ubicación física de la agrupación no electrónica.
- El SGDEA debe asegurar que la recuperación de agrupaciones no electrónicas muestre los metadatos de la gestión de documentos tanto para los documentos electrónicos como no electrónicos asociados a ellas.
- El SGDEA debe Incluir características para el control y grabación del acceso a agrupaciones no electrónicas, incluyendo controles basados en la categoría de seguridad, que sean comparables con las características de las agrupaciones electrónicas.

- El SGDEA debe apoyar la búsqueda de agrupaciones no electrónicas proporcionando solicitudes, facilidades para el registro y la comprobación que reflejen la ubicación actual del ítem.
- El SGDEA debe apoyar la impresión y reconocimiento del código de barras para objetos no electrónicos (por ejemplo, documentos, archivos y otros contenedores), debería apoyar otros sistemas de seguimiento para automatizar el ingreso de datos para seguir el movimiento de tales documentos no electrónicos.
- El SGDEA debe apoyar la conservación y los protocolos de disposición y rutinariamente aplicarlos a los elementos electrónicos y no electrónicos dentro de las agrupaciones híbridas.
- El SGDEA debe asegurar que a un documento no electrónico se le asigna la misma categoría de seguridad que un documento electrónico asociado dentro de una agrupación de documentos híbrida.
- El SGDEA debe permitir diligenciar metadatos de ubicación, que luego van a permitir su ubicación a nivel de unidades documentales, para el caso de los expedientes híbridos.

2.3.3.2. Workflow- Flujos de Trabajo

- El SGDEA debe permitir la creación, administración y ejecución de flujos.
- El SGDEA debe permitir diagramar y modelar flujos electrónicos.
- El SGDEA debe permitir diagramar tareas que componen un proceso y/o procedimiento.
- El SGDEA debe permitir parametrizar los tiempos de ejecución y respuesta de los procesos ejecutados.
- El SGDEA debe permitir incorporar un mecanismo de simulación para analizar los flujos de trabajo modelados.
- El SGDEA debe permitir la administración y control de los procesos por lotes y los procesos automáticos programados.
- El SGDEA debe permitir parametrizar los accesos, creación, modificación o control total para usuarios o grupos de usuarios de los flujos de trabajo.
- El SGDEA no debe limitar el ingreso de acciones que componen cada flujo de trabajo.
- El SGEDEA debe permitir contener múltiples versiones de un mismo proceso y/o procedimiento. Debe permitir al administrador seleccionar la última versión.
- El SGDEA debe generar una trazabilidad de las acciones de los flujos de trabajo e incluirla en las pistas de auditoría.
- El SGDEA debe permite definir los flujos de trabajo basado en plantillas.

2.3.3.3. Requisitos técnicos y operativos adicionales del Sistema

- La solución tecnológica debe tener soporte nativo de IPv6.
- Todos los requisitos de licenciamiento deben ser provistos por el contratista y estar debidamente registrados ante DNDA a nombre la Gobernación de Bolívar.
- Todo el Hardware debe ser provisto por la empresa o contratista que para la implementación del sistema defina la Gobernación de Bolívar.

- Cualquier desarrollo adicional hará parte integral de las funcionalidades del sistema por lo que se establece como inconvenientes previstos para el cumplimiento del objeto a desarrollar sin prejuicio alguno para la Gobernación.
- Es importante que para el desarrollo e implementación del sistema se debe cumplir con la elaboración y firma de los acuerdos de confidencialidad; teniendo en cuenta que existe información sensible y restringida para el conocimiento de la ciudadanía o cualquier actor interesado.
- Todo el proceso de la evaluación de las funcionalidades y requerimientos específicos referentes al sistema debe basarse en el listado de condiciones técnicas plasmadas en el presente documento; por lo cual se recomienda la generación pruebas operativas en producción, con el propósito de validar que sistema propuesto se ajuste a las condiciones y gestiones funcionales institucionales.