

Carrera 89ª #64C-30 Álamos Zona Industrial, Bogotá D.C
contacto@insor.gov.co
Tel: (601) 439 12 21

1. INTRODUCCIÓN

Las entidades públicas en Colombia deben garantizar la utilización de repositorios digitales confiables como parte de la implementación de su Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA). Estos repositorios constituyen la base para asegurar la preservación a largo plazo de los documentos y expedientes electrónicos de archivo, en concordancia con los tiempos de retención definidos en las Tablas de Retención Documental (TRD).

El modelo de requisitos establece que la estructura de almacenamiento de los documentos electrónicos debe responder al Cuadro de Clasificación Documental, garantizando orden, coherencia y trazabilidad en la gestión de la información. Asimismo, la entidad debe implementar una estructura de metadatos que permita la producción, registro, clasificación, acceso, conservación y valoración documental en el tiempo, asegurando que cada documento mantenga de manera permanente la relación entre su contexto, estructura y contenido.

De igual forma, el acceso a los documentos electrónicos de archivo debe articularse con las políticas institucionales de seguridad de la información y con los lineamientos para la publicación de datos abiertos, de manera que se garantice un equilibrio entre transparencia y protección. A su vez, los repositorios deben incorporar mecanismos de seguimiento, control y monitoreo, mediante herramientas y metodologías de auditoría que aseguren su confiabilidad y fortalezcan la preservación digital a largo plazo.

Así las cosas, cada entidad debe adoptar políticas y procedimientos documentados que permitan la preservación, migración o actualización de la información conforme a normas técnicas y estándares reconocidos. De esta forma, se asegura que los documentos electrónicos de archivo conserven su autenticidad, integridad y disponibilidad, consolidando así el patrimonio documental electrónico del Estado colombiano.

En este contexto, el presente documento introduce el modelo de requerimientos funcionales y no funcionales esenciales para la implementación de un Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA). Para su formulación, se tomó como referencia la Guía del Archivo General de la Nación titulada *"Implementación de un Sistema de Gestión de Documentos Electrónicos de Archivo"*, la cual orienta sobre la necesidad de estructurar estrategias de integración que permitan aplicar y controlar de manera efectiva cada una de las etapas de la gestión documental: creación, mantenimiento, difusión y administración. Asimismo, se consideraron normas internacionales como el Modelo Europeo de Requerimientos (MoReq) y las publicaciones del Consejo Internacional de Archivos relacionadas con registros electrónicos, con el propósito de fortalecer la identificación de requisitos que soporten la gestión de los documentos electrónicos de archivo. De igual manera, se incorporó la normatividad colombiana vigente, en particular el Acuerdo 001 de 2024, mediante el cual se establece el Acuerdo Único de la Función Archivística, se definen los criterios técnicos y jurídicos para su implementación en el Estado colombiano y se fijan disposiciones complementarias.

Para completar la integración de este modelo de requisitos, es fundamental considerar los elementos esenciales del Marco de Referencia de Arquitectura Empresarial en Colombia, el principal instrumento del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) para orientar a las entidades públicas en su proceso de transformación digital y en la adopción de buenas prácticas de gestión documental. De este modo, se fortalece la estructura del Sistema de Gestión de Documentos Electrónicos, asegurando que su implementación responda a los retos de la era digital y a las exigencias normativas vigentes en el país.

2. OBJETIVO

El objetivo principal del documento es establecer un modelo de requerimientos funcionales y no funcionales esenciales para la implementación de un Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA) en la entidad, a partir de los lineamientos técnicos y normatividad vigentes en Colombia.

2.1 OBJETIVOS ESPECÍFICOS

- Definir lineamientos para el uso de repositorios digitales confiables alineados con el SGDEA.
- Establecer la estructura de almacenamiento y metadatos que garantice el orden, coherencia, trazabilidad y preservación a largo plazo de los documentos electrónicos de archivo.
- Integrar políticas de acceso, seguridad de la información y publicación de datos abiertos en la gestión documental digital.
- Orientar la adopción de herramientas de seguimiento, control, monitoreo y auditoría para la confiabilidad y preservación digital.
- Promover la aplicación de normas técnicas, procedimientos, y estándares reconocidos para migración y actualización de información.
- Incorporar elementos de normatividad nacional e internacional, incluyendo el Marco de Referencia de Arquitectura Empresarial en Colombia y el Acuerdo 001 de 2024.

3. ALCANCE

Este documento establece los requisitos funcionales y no funcionales necesarios para la gestión y preservación de documentos electrónicos de archivo, constituyendo los lineamientos para la implementación de un Sistema de Gestión de Documentos Electrónicos (SGDEA). Dicho sistema debe abarcar la totalidad de los documentos producidos y recibidos por la entidad, garantizar el cumplimiento de la normatividad vigente en Colombia, adoptar estándares nacionales e internacionales y alinearse con el Marco de Referencia de Arquitectura Empresarial del MinTIC.

4. MARCO NORMATIVO

- Ley 594 de 14 de julio de 2000. Ley General de Archivos.

- Ley 1712 de 06 de marzo de 2014. Por medio de la cual se crea la Ley de transparencia y el derecho de acceso a la información pública nacional y se dictan otras disposiciones.

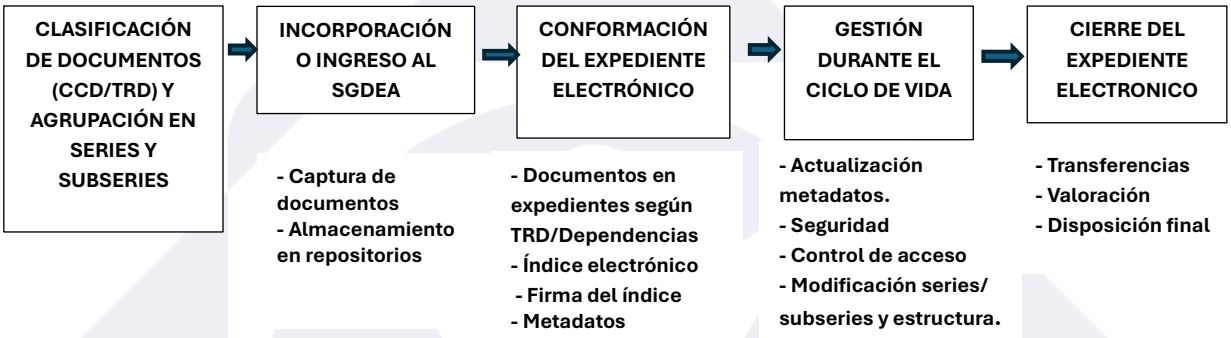
- Decreto 1080 de 26 de mayo de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura.

- Acuerdo 001 de 2024. Archivo General de la Nación. (2024, 10 de abril). *Acuerdo 001 de 2024. Diario Oficial No. 52.723.* Por el cual se establece el Acuerdo Único de la Función Archivística, se definen los criterios técnicos y jurídicos para su implementación en el Estado colombiano y se fijan otras disposiciones. Bogotá: AGN.

5. REQUISITOS

5.1. REQUISITOS BÁSICOS DEL SISTEMA.

Se refieren a las funciones mínimas que debe tener un sistema de gestión de documentos electrónicos (SGDEA): garantizar la captura de documentos, asignarles un identificador único, vincular metadatos obligatorios y asegurar que los registros sean íntegros, auténticos e inalterables.



CAPTURA DE DOCUMENTOS ELECTRÓNICOS: La incorporación de documentos al Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA) comprende cuatro acciones principales: registro, clasificación, asignación de metadatos y almacenamiento. Todo documento elaborado o recibido se convierte en documento de archivo en el momento en que es capturado en el sistema. En esta captura, los documentos se clasifican mediante códigos definidos en el cuadro de clasificación documental de la entidad. Los aspectos a tener en cuenta son los siguientes:

Registro: Ingresar el documento al sistema.
Clasificación: Asignar código según el cuadro de clasificación documental.
Metadatos: Completar la información requerida para su identificación y gestión.
Almacenamiento: Guardar el documento en el repositorio correspondiente.

Al incorporar documentos en el SGDEA se debe garantizar su conservación física y digital, mantener el contenido estable sin cambios no autorizados y aplicar controles de acceso para protegerlos de usuarios no permitidos. También es necesario verificar la validez de las copias y copias autenticadas, realizar la captura de componentes digitales (por ejemplo, archivos multimedia) y conformar expedientes electrónicos completos, organizados de acuerdo con las series y subseries documentales definidas por la entidad.

REGISTRO ÚNICO E INALTERABLE: Cada documento que ingresa al SGDEA se registra una sola vez y queda protegido contra modificaciones no autorizadas. Esto garantiza integridad, autenticidad y trazabilidad. *Ejemplo:* Un informe financiero trimestral se captura en el sistema como documento único; cualquier consulta futura mostrará siempre la misma versión, y cualquier acción realizada (como revisión o transferencia a archivo central) queda registrada en el historial del documento.

GENERACIÓN Y VINCULACIÓN DE METADATOS: Al incorporarse un documento, el SGDEA genera y asocia metadatos que describen su contenido, origen, fecha, responsable y categoría, facilitando su identificación y gestión. Los metadatos estandarizados son los siguientes, pero la entidad puede crear otro tipo de metadatos

5.2 CLASIFICACIÓN Y ORGANIZACIÓN

El sistema debe permitir la creación de estructuras jerárquicas (series y subseries), apertura y cierre de expedientes, y su vinculación a un cuadro de clasificación documental. Esto asegura que los documentos estén organizados de manera coherente y rastreable en todo su ciclo de vida.

- Creación y gestión de series/subseries: parametrización que permita realizar modificaciones según las reestructuraciones que se presenten en la entidad en todos sus niveles.
- Organización jerárquica de expedientes: siguiendo la estructura de sección / subsección / serie / subserie según el organigrama de la entidad.
- Reglas de apertura/cierre: están relacionadas con las fases de archivo de gestión, central e histórico.
- Asociación a planes de clasificación: se debe implementar las TRD de la entidad.

5.3 GESTIÓN DE METADATOS

Cada documento y expediente debe contar con un conjunto mínimo de metadatos obligatorios (identificación, contexto, fecha, productor, etc.). El sistema debe permitir ampliar este esquema según necesidades de la entidad, garantizando que algunos metadatos esenciales permanezcan inalterables.

- **Metadatos de contenido**

a) **Tipo de recurso de información:** Clasificación general del documento según su naturaleza (texto, imagen, audio, multimedia, etc.).
b) **Tipo documental:** Especificación del tipo de documento según la tipología institucional (informe, resolución, acta, memorando, oficio, etc.).
c) **Título del documento:** Nombre o encabezado que identifica el contenido del documento.
d) **Responsables y emisores:** Autor o emisor del contenido, destinatario, responsable de proyectar el contenido, entidad que respalda el documento, y persona o sistema desde donde se crea.
e) **Clasificación de acceso:** Nivel de acceso o restricción del documento según políticas de seguridad y confidencialidad.
f) **Fechas relevantes:** Fecha de creación, transmisión y recepción del documento.
g) **Folio:** Identificación electrónica que permite localizar el documento dentro del sistema.
h) **Tema o asunto administrativo:** Trámite o proceso al que se vincula el documento.
i) **Palabras clave:** Términos que describen el contenido y facilitan la búsqueda y recuperación.

- **Metadatos de estructura**

a) **Descripción:** Breve síntesis que explica el contenido y propósito del documento.
b) **Formato:** Tipo de archivo o soporte físico (PDF, Word, papel, etc.).
c) **Estado:** Situación actual del documento (borrador, aprobado, archivado, vigente, etc.).
d) **Proceso administrativo:** Trámite, actuación o procedimiento al que pertenece.

e) **Unidad administrativa responsable:** Dependencia encargada de generar, custodiar o gestionar el documento.
f) **Perfil autorizado:** Usuarios o roles que pueden acceder, modificar o aprobar el documento.
g) **Ubicación:** Localización física o lógica dentro del sistema o repositorio.
h) **Serie/Subserie documental:** Clasificación según el cuadro de series y subseries adoptado por la entidad.

- **Metadatos de contexto**

a) **Jurídico-administrativo:** Normas, leyes, resoluciones o disposiciones que respaldan o regulan el documento.
b) **Documental:** Relación con otros documentos, expediente o serie a la que pertenece.
c) **De procedencia:** Origen o unidad productora del documento.
d) **Procedimental:** Etapa del proceso o trámite en la que se generó el documento.
e) **Tecnológico:** Requisitos técnicos o sistemas utilizados para crear, almacenar o gestionar el documento.

5. 4. CONTROL DE ACCESO Y SEGURIDAD.

Incluye la definición de usuarios, roles y permisos, de manera que solo las personas autorizadas accedan a determinados documentos o expedientes. Además, debe existir un registro de auditoría que documente quién accedió, modificó o gestionó cada registro, con mecanismos de autenticación y trazabilidad.

De conformidad con lo establecido en el Capítulo 1 sobre *acceso y control de documentos* del Título 7 del Acuerdo 001 de 2024, se presenta los lineamientos esenciales para garantizar la disponibilidad, clasificación, reserva y conservación de los documentos de archivo, asegurando un acceso seguro y conforme a la normativa vigente:

- **Acceso a los documentos de archivo (Artículo 7.1.1)**

- Identificar los documentos de archivo, ya sea en soporte físico o electrónico.
- Verificar el marco legal aplicable sobre acceso a la información.
- Clasificar los documentos según correspondan como:
    - Información pública
    - Información clasificada
    - Información reservada
- Registrar esta clasificación en el **"Índice de Información Clasificada y Reservada"**.
- Asegurar la articulación de esta información con los demás instrumentos de gestión de la información pública.

- **Disponibilidad y accesibilidad de documentos electrónicos (Artículo 7.1.2)**

- Mantener los documentos electrónicos y sus metadatos disponibles para los grupos de interés.
- Establecer niveles de acceso conforme a la **Ley 1712 de 2014** o normas que la modifiquen o sustituyan.
- Garantizar en todo momento:

- **Autenticidad** del documento
- **Fiabilidad**
- **Integridad**

- Asegurar que los documentos se mantengan accesibles a lo largo de su ciclo vital, independientemente del sistema de gestión utilizado.

Los formatos deben ser abiertos, libres y accesibles. Además, para documentos con firma electrónica, estampas o sellos digitales, ofrecer mecanismos de verificación de autenticidad al interesado.

➢ **Reserva de la información (Artículo 7.1.3)**

- Verificar qué información está sujeta a reserva y cuál no.
- Elaborar versiones públicas que mantengan la reserva de datos personales o sensibles.

- **Criterios mínimos de reserva (Parágrafo 1):**
  - La reserva aplica solo al contenido, no a la existencia del documento.
  - Solo se reserva información que comprometa derechos fundamentales o bienes constitucionales; los procesos o actuaciones no se restringen.
  - La reserva es temporal, según lo determinado por la Ley.

- **Versiones públicas (Parágrafo 2):**
  - Aplicar estándares de anonimización de datos.
  - Identificar claramente los datos a anonimizar según normativa de protección de datos personales.
  - Garantizar que la información sea utilizable para fines públicos sin comprometer la privacidad o confidencialidad.

➢ **Restricciones de acceso a documentos originales por conservación (Artículo 7.1.4)**

- Determinar si el acceso a los documentos originales debe restringirse por razones de conservación.
- Mantener disponible la **información contenida**, mediante técnicas de reproducción adecuadas.

Es de anotar, que la restricción debe basarse en evaluación por personal especializado en conservación-restauración.

5.5. GESTIÓN DEL CICLO DE VIDA.

Se deben establecer plazos de retención de documentos, así como procedimientos para su transferencia, conservación o eliminación definitiva.

Según lo establecido en el acuerdo 001 de 2024, tener en cuenta lo siguiente.

➢ **Criterios de valoración documental (Artículo 5.2)**

- **Definir criterios**

  - Analizar el contexto, funciones y procedimientos de la entidad.
  - Establecer los criterios desde la planificación de la producción documental y plasmarlos en las TRD.

- **Tiempos de retención**

  - Determinar según el valor administrativo, legal, jurídico, contable o técnico de los documentos.
  - Sustentar en normas jurídicas vigentes.
  - Parametrizar los tiempos de las TRD de la entidad.

- **Disposición final.** Establecer la parametrización según los dispuesto en el capítulo 5 *Disposición de documento* del acuerdo 001 de 2024, así:

  - **Conservación total (CT)** *(Art. 4.5.2)*: Identificar en las TRD o TVD las series y subseries con disposición final "Conservación Total". Además, garantizar su preservación considerando sus valores históricos, socioculturales, científicos o estéticos.
  - **Selección (S)** *(Art. 4.5.3)*. Determinar qué series o subseries de gran volumen o información duplicada requieren selección, así como el tamaño de muestra y métodos de selección adecuados, danto prioridad de conservación a las series con valor permanente.
  - **Eliminación (E)** *(Art. 4.5.4)*. aplicar la eliminación o borrado electrónico a los documentos que según las TRD tienen esta disposición final.

5.6. GESTIÓN DE EXPEDIENTES ELECTRÓNICOS

Teniendo en cuenta la sección 2 sobre expediente electrónico del acuerdo 001 de 2024, para la conformación y gestión de expedientes electrónicos de archivo se resaltan los siguientes escenarios:

➢ **Inicio del trámite o procedimiento** *(Art. 4.3.2.1)*

- Identificar el trámite, actuación o procedimiento que generará documentos.
- Elaborar el Modelo de Requisitos de Documentos Electrónicos de Archivo, siguiendo los lineamientos del Archivo General de la Nación.

➢ **Clasificación y organización de documentos** *(Art. 4.3.2.1, parágrafo 2)*

- Clasificar los documentos según el Cuadro de Clasificación Documental (CCD) y las Tablas de Retención Documental (TRD).

- Respetar el principio de orden original y agrupar los documentos en series y subseries documentales, sin importar su formato o tipo de información.

➢ **Incorporación al SGDEA** *(Art. 4.3.2.1)*

- Capturar todos los documentos generados en el SGDEA desde el inicio hasta la finalización del trámite.
- Almacenar los documentos en **repositorios digitales de confianza**, garantizando la seguridad de la información.

➢ **Elementos del expediente electrónico** *(Art. 4.3.2.2)*

- Incluir **todos los documentos electrónicos de archivo** del trámite.
- Generar un **índice electrónico** del expediente.
- Firmar digitalmente el índice para garantizar **autenticidad e integridad**.
- Asociar **metadatos** de contenido, estructura, contexto y otros definidos por la entidad, asegurando su actualización durante todo el ciclo de vida de los documentos.

➢ **Finalización y disposición** *(Art. 4.3.2.1)*

- Completar el expediente electrónico con todos los documentos generados.
- Mantener el acceso y conservación según las políticas de la entidad hasta su disposición final o prescripción.

5.7 BÚSQUEDA Y RECUPERACIÓN

El sistema debe ofrecer búsquedas simples y avanzadas, tanto por metadatos como por contenido. Además, debe permitir la exportación de resultados y la visualización íntegra de documentos y expedientes, garantizando acceso rápido y confiable a la información. Aspectos a destacar:

- Configurar campos de búsqueda y permisos (administrador).
- Indexar metadatos y contenido en todos los niveles (clase, agrupación, volumen, documento).
- Habilitar búsqueda única con autocompletar.
- Permitir consultas combinadas: booleanos, coincidencias aproximadas, comodines, rangos de fechas, formatos, códigos de clasificación, palabras clave, identificador único y nombre.
- Buscar en una o varias agrupaciones, incluidas híbridas (electrónicas/no electrónicas).
- Mostrar total de resultados y listado navegable (miniaturas); ver expedientes y documentos relacionados; abrir con un clic según acceso.
- Clasificar y refinar resultados (relevancia, fecha, autor, tipo, tamaño) y permitir “buscar dentro de resultados”.
- Previsualizar sin descargar ni usar software externo; reproducir audio/video.
- Garantizar seguridad: nunca revelar contenido ni metadatos restringidos.
- Permitir recuperar y mostrar como unidad todos los documentos y metadatos de una agrupación o volumen.

5.8 INTEROPERABILIDAD Y TRANSFERENCIA

El sistema debe poder intercambiar información con otros sistemas (nacionales o internacionales) mediante exportación e importación de documentos y metadatos. También debe permitir la transferencia de expedientes completos a otras entidades, usando estándares reconocidos (como XML, METS, Dublin Core). Para las entidades públicas y siguiendo en Marco de Referencia de Arquitectura Empresarial del Ministerio de Tecnología e Información Mintic, a continuación se presenta los pasos a tener en cuenta con enfoque de este marco:

➢ **Diagnóstico de interoperabilidad**

- Evaluar el estado actual de los sistemas de gestión documental y su capacidad de interoperar con otros sistemas institucionales y externos.
- Identificar brechas en estándares, formatos y procesos que puedan afectar la interoperabilidad.
- Analizar cómo la gestión documental se integra con la misión, visión y objetivos estratégicos de la entidad.

➢ **Definición de procesos y metadatos interoperables**

- Establecer procesos documentales y estructuras de expedientes compatibles con normas de interoperabilidad y requisitos del MoReq.
- Definir metadatos estandarizados que permitan la intercambiabilidad de información entre sistemas.
- Garantizar que los documentos electrónicos puedan ser interpretables y reutilizables por diferentes aplicaciones y plataformas.

➢ **Integración con la Arquitectura Empresarial**

- Alinear los elementos documentales con las capas de la Arquitectura Empresarial, considerando la interoperabilidad como principio transversal:

  - **Capa estratégica:** Vincular interoperabilidad con los objetivos institucionales y políticas de gobierno digital.
  - **Capa de procesos:** Incorporar la gestión documental interoperable en todos los procesos clave.
  - **Capa de información:** Asegurar que la información cumpla con estándares abiertos y formatos accesibles.
  - **Capa de aplicaciones:** Seleccionar o adaptar sistemas que soporten intercambio seguro de datos entre plataformas.
  - **Capa tecnológica:** Garantizar infraestructura que permita interoperabilidad continua, preservación digital y seguridad.

➢ **Diseño e implementación del SGDEA interoperable**

- Implementar el **Sistema de Gestión Documental y de Expedientes Electrónicos (SGDEA)** garantizando:
  - Interoperabilidad con otros sistemas internos y externos.
  - Seguridad y preservación digital de los documentos.
  - Trazabilidad y auditoría de todas las acciones sobre los documentos.

- Asegurar que el SGDEA funcione como **parte integral del ecosistema institucional**, no como un sistema aislado.

5. 9. PRESERVACIÓN DIGITAL

Se enfoca en garantizar el acceso a largo plazo. Incluye migración de formatos para evitar la obsolescencia tecnológica, soporte de firmas digitales y sellos de tiempo, control de versiones de los documentos, y mecanismos de almacenamiento seguro con copias de respaldo.

- **Criterios para la preservación digital (Art. 6.1.3.3)**

Para definir los criterios de preservación digital, cada entidad debe analizar su contexto organizacional, sus funciones y los procedimientos que generan los documentos electrónicos. Los pasos clave son:

- Identificar flujos de información relevantes dentro de la entidad.
- Caracterizar los documentos electrónicos que deben preservarse según su valor y uso.
- Evaluar estrategias de preservación, considerando recursos, tecnología y normatividad.
- Cumplir con los tiempos de retención documental establecidos en las TRD o TVD.
- Asegurar que los documentos sean interpretables, recuperables y protegidos, independientemente del formato o soporte electrónico.

- **Evaluación de riesgos (Art. 6.1.3.4)**

La preservación digital debe considerar los riesgos que podrían afectar la disponibilidad y fiabilidad de los documentos electrónicos. Los riesgos mínimos incluyen:

- Obsolescencia o degradación de soportes físicos.
- Obsolescencia de formatos, software y hardware.
- Desastres naturales o eventos accidentales.
- Ataques deliberados, fallas organizacionales o errores humanos.

Evaluar estos riesgos permite formular un **Plan de Preservación Digital a Largo Plazo** que minimice pérdidas y garantice la continuidad de la información.

- **Estrategias de preservación digital (Art. 6.1.3.5)**

Las estrategias técnicas aseguran que los documentos puedan ser conservados y consultados a futuro:

- **Migración:** Cambio de plataformas, hardware o software a entornos actuales.
- **Conversión:** Transformación de documentos de un formato a otro, según necesidades de preservación o consulta.
- **Emulación:** Recreación del entorno original de hardware y software para leer formatos obsoletos.
- **Refreshing:** Transferencia de datos a otro soporte sin alterar el contenido.

Adicionalmente, para evidencia de la creación o actualizaciones, se debe:

- Documentar y justificar la estrategia seleccionada.
- Registrar todas las acciones de gestión y administración de los documentos digitales.
- Mantener vigilancia sobre desarrollos tecnológicos, técnicas de migración y conversión, y normas técnicas aplicables.

- Establecer un esquema de metadatos adecuado y asegurar su almacenamiento.

➢ **Procesos y procedimientos (Art. 6.1.3.6)**

El Plan de Preservación Digital a Largo Plazo debe incluir todos los procesos y procedimientos necesarios para garantizar la cadena de preservación digital durante todo el ciclo vital de los documentos. Aspectos clave a considerar:

- Gestión de documentos digitalizados y nativos digitales desde la planeación y valoración documental.
- Cronograma de transferencias y eliminación según TRD/TVD.
- Selección de formatos, medios y soportes seguros.
- Metadatos asociados y acciones para garantizar fiabilidad y autenticidad.
- Cumplimiento de normas legales y reglamentarias, incluyendo auditorías y vigilancia tecnológica.
- Identificación y mitigación de riesgos de obsolescencia tecnológica.

5.10 Auditoría y trazabilidad

Cada acción ejecutada sobre un documento o expediente, desde su creación hasta su eventual eliminación, debe quedar detalladamente registrada y gara su trazabilidad. Es fundamental que el registro incluya el historial completo de accesos, modificaciones, transferencias y autorizaciones, permitiendo reconstruir fielmente el ciclo de vida documental. Para ello, los informes de auditoría deben protegerse contra alteraciones no autorizadas, empleando mecanismos como firmas digitales, cifrado y redundancia en el almacenamiento de logs.

- Registro de eventos: Toda interacción con el documento queda registrada, incluyendo fechas, responsables y naturaleza de la acción.
- Trazabilidad completa: Se puede seguir el recorrido del documento desde su origen hasta su destino final, evidenciando cada etapa procesal.
- Informes de auditoría: Los reportes generados permiten supervisar el cumplimiento de los procedimientos y detectar posibles anomalías.
- Protección de logs: Los registros de trazabilidad están resguardados contra manipulación y pérdidas, reforzando la fiabilidad del sistema.

5.11. REQUISITOS NO FUNCIONALES

Los requisitos no funcionales representan las condiciones esenciales de calidad que debe garantizar el sistema para cumplir adecuadamente su propósito y asegurar la confianza de quienes interactúan con él. Entre estos requisitos se encuentran el rendimiento, la escalabilidad, la usabilidad, la alta disponibilidad, el cumplimiento normativo y la seguridad informática.

- Escalabilidad y rendimiento: El sistema debe ser capaz de adaptarse al crecimiento en la cantidad de usuarios, documentos y transacciones, manteniendo tiempos de respuesta óptimos y eficiencia operativa, sin degradar su funcionamiento a medida que aumenta la demanda.

- Usabilidad: Es fundamental que la interfaz resulte intuitiva, accesible y fácil de utilizar para todas las personas usuarias, permitiendo la gestión ágil de los documentos electrónicos y reduciendo la curva de aprendizaje.

- Alta disponibilidad: El sistema debe estar disponible de manera continua, minimizando los tiempos de inactividad y garantizando el acceso confiable a la información en cualquier momento. Para ello, es indispensable la implementación de infraestructuras redundantes y mecanismos de recuperación ante fallos.
- Cumplimiento normativo: Es imprescindible que la solución tecnológica cumpla con las leyes, regulaciones y estándares nacionales e internacionales relacionados con la gestión documental, la protección de datos y la interoperabilidad entre sistemas.
- Seguridad informática: La protección de la información y de los procesos asociados implica el uso de técnicas avanzadas como el cifrado de datos, la autenticación robusta, la realización periódica de copias de seguridad y la definición de planes de contingencia frente a incidentes. Asimismo, deben establecerse controles que prevengan accesos no autorizados y garanticen la confidencialidad, integridad y disponibilidad de los documentos.

1. ARTICULACIÓN ENTRE MOREQ Y ARQUITECTURA EMPRESARIAL

La implementación del Modelo de Requisitos para la Gestión de Documentos Electrónicos – MoReq, en articulación con la Arquitectura Empresarial del Estado Colombiano, constituye un componente estratégico en la consolidación de los Sistemas de Gestión Documental y de Expedientes Electrónicos (SGDEA) dentro de las entidades públicas. Esta integración permite garantizar que los documentos electrónicos conserven su autenticidad, integridad, disponibilidad e interoperabilidad a lo largo de todo su ciclo de vida, en cumplimiento de los lineamientos establecidos por el Archivo General de la Nación (AGN), la Política de Gobierno Digital y el Modelo Integrado de Planeación y Gestión (MIPG).

El proceso de implementación se desarrolla en varias etapas interdependientes. En primer lugar, las entidades realizan un diagnóstico de la situación actual de su gestión documental, identificando fortalezas, debilidades y el estado de sus sistemas de información asociados. A partir de esta información, se definen los procesos, estructuras documentales y metadatos de acuerdo con los requisitos del MoReq y las disposiciones normativas del AGN, con el fin de establecer una base técnica y normativa uniforme. Posteriormente, se lleva a cabo la alineación de estos elementos con las capas de la Arquitectura Empresarial —estratégica, procesos, información, aplicaciones y tecnología—, asegurando que la gestión documental no se conciba como un proceso aislado, sino como parte integral del modelo de gestión institucional.

En la fase siguiente, las entidades diseñan e implementan el SGDEA bajo criterios de seguridad, interoperabilidad y preservación digital, incorporando mecanismos de trazabilidad, auditoría y control que fortalezcan la transparencia en la gestión pública. Una vez consolidado el sistema, se desarrollan programas de capacitación y sensibilización dirigidos a los funcionarios responsables de su uso, con el propósito de garantizar la apropiación institucional y el cumplimiento de los estándares de calidad.

Finalmente, se establecen procesos de monitoreo, auditoría y mejora continua, que permiten evaluar periódicamente la eficacia del sistema, introducir ajustes necesarios y asegurar la sostenibilidad en el tiempo. De esta forma, la aplicación conjunta del Modelo de Requisitos y de la Arquitectura Empresarial no solo fortalece la gestión documental electrónica en las entidades públicas colombianas, sino que también contribuye

a la modernización del Estado, a la eficiencia administrativa y al acceso oportuno y confiable de la información por parte de la ciudadanía.

A continuación, se incorpora las actividades en materia de gestión documental dentro de los dominios de la Arquitectura empresarial:

Arquitectura de Negocio: Integrar los procesos archivísticos en el mapa de procesos institucional y con el Modelo Integrado de Planeación y Gestión (MIPG).

Arquitectura de Información: Definir un banco terminológico y metadatos conforme al modelo de requisitos, los cuales deben estar relacionados en el cuadro de clasificación documental con el inventario de datos. También alineados con los instrumentos archivísticos de la entidad.

Arquitectura de Aplicación: En el marco de la Arquitectura Empresarial del Estado, el SGDEA debe garantizar el cumplimiento de los requisitos definidos en el modelo MoReq —captura, control de acceso, auditoría e interoperabilidad—, asegurando su integración con los sistemas institucionales clave. Estos lineamientos de la arquitectura de aplicación permiten consolidar la interoperabilidad y el intercambio de información entre las entidades públicas, en concordancia con las directrices del MinTIC para la gestión documental electrónica y la articulación con los demás dominios de la Arquitectura Empresarial.

Arquitectura Tecnológica: Diseñar infraestructura segura y escalable, adoptando estándares abiertos para la preservación digital a largo plazo.