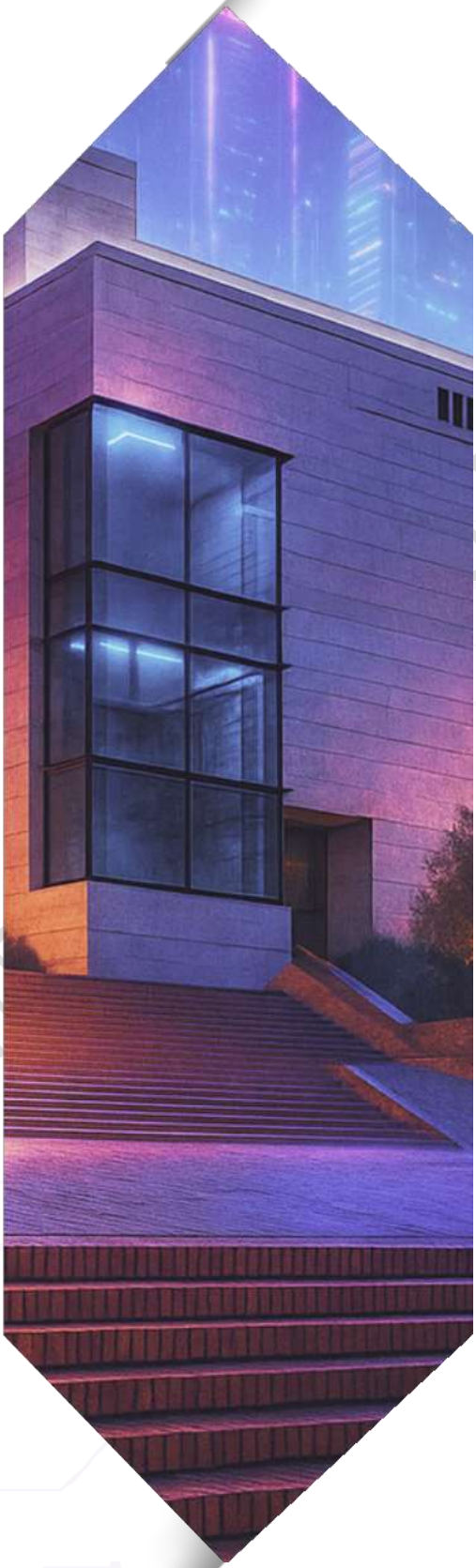
UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

ARCHIVO DE BOGOTÁ
La historia la construimos juntos

3.4.5. MODELO DE REQUISITOS TECNOLOGICOS







PARTE INTEGRAL TÉCNICO

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA GENERAL
BOGOTÁ

CONTROL DE CAMBIOS Y VERSIONAMIENTO DEL DOCUMENTO

Proyecto: Realizar el diagnóstico de los fondos y colecciones documentales digitales y sus medios de almacenamiento en el Archivo General de Bogotá. El diagnóstico de la producción electrónica de documentos históricos en 12 entidades del distrito y la definición de la arquitectura tecnológica para soportar el proyecto de preservación digital.			
Documento: 3.4.5. Modelo de Requisitos Tecnológicos			
Área involucrada: Subdirección de Gestión del Patrimonio Documental del Distrito.			
Versión	**Descripción de cambios**	**Autor**	**Fecha creación**
1.0	Primera versión para validar por parte del Archivo General de Bogotá.	Universidad Distrital	21 de noviembre del 2025
2.0	Ajustes solicitados por el Archivo General de Bogotá.	Universidad Distrital	15 de diciembre del 2025

PARTE INTEGRAL DEL ANEXO TÉCNICO

TABLA DE CONTENIDO

I. PRESENTACIÓN 5
II. CONTEXTO ESTRATÉGICO DE LAS DIRECTRICES 8
2.1 Contexto institucional 8
2.2 Marco normativo y de política pública 9
2.3 Articulación institucional y tecnológica 9
III. ENFOQUE Y METODOLOGÍA 12
3.1 Enfoque general 12
3.2 Estructura metodológica 13
IV. MODELO DE REQUISITOS TECNOLÓGICOS 17
4.1 Objetivo del Modelo de Requisitos Archivo General de Bogotá. 17
4.2 Alcance 17
4.3 Requisitos Funcionales 18
R1. Estructura del paquete de información 20
R2. Requisitos para la admisión 22
R3. Requisitos para la creación de Paquetes de Información de Archivo (PIA) 24
R4. Requisitos de Planificación de la Preservación 27
R5. Requisitos de almacenamiento y preservación 28
R6. Gestión de la Información Descriptiva 30
R7. Requisitos para la generación, control y distribución de Paquetes de información de Consulta (PIC) 32
R8. Seguridad y Administración de Paquetes 33
4.4 Requisitos No Funcionales 35
R9. Seguridad 35
R10. Auditoría y Trazabilidad 36
R11. Disponibilidad, Eficiencia Operativa e Interoperabilidad 36
R12. Interfaz, Configuración y Administración 37
R13. Reportes, Estándares y Almacenamiento 38
R14. Integración, Sincronización y Operación en Tiempo Real 38
R15. Escalabilidad, Arquitectura y Compatibilidad 39
R16. Interoperabilidad Avanzada y Comunicación Institucional 39
R17. Rendimiento 40
R18. Síntesis ampliada de los requisitos complementarios 40
4.5 Plan de acción y ruta de implementación 41

PARTE INTEGRAL DEL ANEXO TÉCNICO

V. RECURSOS Y SOSTENIBILIDAD 43
5.1 Presupuesto estratégico 43
5.2 Sostenibilidad institucional y tecnológica 44
VI. SEGUIMIENTO, EVALUACIÓN E IMPACTO 45
6.1 Mecanismos de evaluación y revisión 45
6.2 Impacto esperado 46
VII. NOTAS ACLARATORIAS 48
REFERENCIAS 52

PARTE INTEGRAL DEL ANEXO TÉCNICO

I. PRESENTACIÓN

La consolidación de un Repositorio Archivístico Digital Confiable[1] para el Archivo General de Bogotá constituye un eje estructural dentro del proyecto de fortalecimiento de la memoria histórica y del patrimonio documental digital del Distrito. Este repositorio no solo funciona como soporte tecnológico, sino como parte integral del Sistema Institucional de Archivos, en el cual convergen los procesos de gestión, preservación y acceso a los documentos electrónicos de archivo, garantizando su autenticidad, integridad, disponibilidad y accesibilidad a largo plazo.

El análisis realizado sobre los fondos y colecciones documentales digitales incluyendo la extracción de metadatos, la validación técnica de formatos, la revisión de integridad y la correlación con instrumentos de descripción archivística confirma la necesidad de una infraestructura estandarizada y robusta que permita enfrentar los desafíos actuales y futuros de la preservación digital. La evidencia documentada en el informe 3.1.3 muestra que el Archivo General de Bogotá administra un volumen significativo de activos digitales (1.450.812 archivos analizados en la muestra) con una predominancia de imágenes fijas en formato TIFF y JPEG, además de materiales textuales, audiovisuales, sonoros y datos estructurados. Esta diversidad demanda capacidades avanzadas de control, interoperabilidad y gestión de riesgos tecnológicos.

En coherencia con estas necesidades, el Archivo General de Bogotá adopta como pilar conceptual el Modelo de Referencia OAIS (NTC-ISO 14721[2]), que establece funciones esenciales para la operación de un repositorio confiable: Ingesta, Almacenamiento Seguro, Gestión de Datos, Administración, Planificación de la Preservación y Acceso. Dichas funciones estructuran el manejo de los paquetes de información de transferencia (PIT)[3] correspondientes al proceso de ingesta, los paquetes de información de Archivo (PIA)[4] correspondientes a la preservación digital y los paquetes de información de consulta (PIC)[5] correspondientes a la difusión o consulta por la comunidad designada, garantizando un tratamiento coherente del documento electrónico y de sus metadatos descriptivos, estructurales y de preservación a lo largo del ciclo de vida.

La implementación del modelo OAIS se complementa con los requisitos de la NTC-ISO 16363[6], orientada a la auditoría de repositorios digitales confiables, que aporta criterios sobre gobierno institucional, políticas de preservación, seguridad, continuidad operativa, mecanismos de verificación de integridad (hash), trazabilidad y administración del riesgo tecnológico. Estos elementos son consistentes con los hallazgos del diagnóstico, en especial la necesidad de fortalecer la normalización de metadatos, la homologación de estructuras de almacenamiento y la incorporación de controles sistemáticos de integridad y perdurabilidad (fixity)[7].

De igual manera, se integran los lineamientos del Acuerdo AGN 001 de 2024, que define las obligaciones para la producción, gestión, transferencia y preservación de documentos electrónicos de archivo, y cuyos criterios fueron aplicados durante las etapas de diagnóstico para el análisis de fondos, colecciones y medios de almacenamiento. Además de las experiencias internacionales de repositorios como

[1] Ver glosario en 3.4.2 Directrices técnicas y normativas
[2] Ver referentes internacionales y nacionales en 3.4.2 Directrices técnicas y normativas
[3] Ver glosario en 3.4.2 Directrices técnicas y normativas
[4] Ver glosario en 3.4.2 Directrices técnicas y normativas
[5] Ver glosario en 3.4.2 Directrices técnicas y normativas
[6] Ver referentes internacionales y nacionales en 3.4.2 Directrices técnicas y normativas
[7] Ver glosario en 3.4.2 Directrices técnicas y normativas

Portico[8], CLOCKSS[9] y LOCKSS[10], así como los lineamientos del Recommended Formats Statement (RFS)[11] y la base PRONOM[12], para reforzar la importancia de adoptar estrategias de redundancia 3-2-1, que se define como una regla de respaldo de datos que consta de tres copias de los datos, dos medios de almacenamiento diferentes y una copia que se guarda fuera del sitio, cuyo objetivo es minimizar el riesgo de pérdida de objetos digitales o metadatos por fallas de hardware, borrados accidentales o desastres.

Se considero importante también el monitoreo permanente de obsolescencia en objetos digitales y medios de almacenamiento, establecer migraciones planificadas, utilizar estrategias básicas de preservación digital como la *bit level preservation* que consiste en mantener los datos originales de un archivo (sus bits) exactamente como están, sin ninguna modificación, manteniendo múltiples copias de seguridad y realizar comprobaciones de integridad como el uso de hashes MD5 para garantizar que el archivo no se corrompa y finalmente el uso de metadatos PREMIS[13], METS[14] y Dublin Core[15] para garantizar una preservación confiable y escalable.

El diagnóstico evidenció brechas estructurales relacionadas con nomenclaturas no estandarizadas, ausencia de correspondencia plena entre los directorios y la jerarquía archivística, duplicidad de archivos, presencia de archivos sin extensión y desafíos para la correlación automática entre instrumentos de descripción y objetos digitales. En el caso de la Colección Armando Matiz, por ejemplo, se logró confirmar parcialmente la correspondencia entre signaturas topográficas e imágenes mediante verificación visual, pero también se identificaron inconsistencias que evidencian la urgencia de fortalecer los procesos archivísticos desde la creación y captura de los objetos digitales.

Por ello, la preservación digital no puede abordarse como una actividad posterior o aislada. Requiere integrarse desde la producción del documento, mediante el uso de formatos abiertos, estructuras normalizadas de expediente electrónico, metadatos completos y controlados, verificación continua de integridad y preparación adecuada de los objetos digitales para transferencias primarias, secundarias y electrónicas.

En este contexto, el Modelo de Requisitos Tecnológicos del Archivo General de Bogotá establece las bases para un repositorio que incorpore:

- Almacenamiento inmutable con controles WORM[16], que garantizan que los metadatos o los objetos digitales, una vez grabados/escritos no pueden ser modificados, ni eliminados hasta que expire el periodo de retención definido, cuando esto aplique;

- Auditorías automáticas de integridad por algoritmos de la familia SHA-2 (SHA-256/SHA-512) que generan una huella digital única (hash) de longitud fija para cualquier dato para el descrito entre paréntesis de 256 o 512 bits,

PARTE INTEGRAL DEL ANEXO TÉCNICO

[8] Ver glosario en 3.4.2 Directrices técnicas y normativas
[9] Ver glosario en 3.4.2 Directrices técnicas y normativas
[10] Ver glosario en 3.4.2 Directrices técnicas y normativas
[11] Ver glosario en 3.4.2 Directrices técnicas y normativas
[12] Ver glosario en 3.4.2 Directrices técnicas y normativas
[13] Ver glosario en 3.4.2 Directrices técnicas y normativas
[14] Ver glosario en 3.4.2 Directrices técnicas y normativas
[15] Ver glosario en 3.4.2 Directrices técnicas y normativas
[16] Ver glosario en 3.4.2 Directrices técnicas y normativas

- Uso de controles sistemáticos de integridad y perdurabilidad (fixity)[17].

- Monitoreo de obsolescencia de formatos y software, utilizando técnicas de preservación digital definidas en la guía técnica GTC-ISO 18492[18];

- Administración estructurada de paquetes de Información de Archivo (PIA), a través del uso de metadatos PREMIS;

- Integración con los instrumentos archivísticos institucionales;

- Mecanismos seguros de acceso y control de permisos basados en políticas institucionales, para el Archivo General de Bogotá las directrices de la Oficina OTIC de la secretaria general;

- Capacidades de automatización para ingesta, validación y control de calidad.

La adopción de este modelo permitirá al Archivo General de Bogotá consolidarse como custodio de la memoria documental digital del Distrito Capital, garantizando la sostenibilidad tecnológica, la continuidad operativa, la transparencia institucional y la protección de los derechos asociados a la información pública.

En suma, el repositorio archivístico digital confiable del Archivo General de Bogotá se concibe como una infraestructura estratégica que articula los marcos normativos, los estándares internacionales, las necesidades reales, así como brechas detectadas en los diagnósticos de fondos y colecciones, medios de almacenamiento y entidad adscrita y las necesidades requeridas a nivel de infraestructura tecnológica y funcional.

Su implementación permitirá transitar hacia un ecosistema de preservación digital integral, auditable y alineado con las mejores prácticas internacionales, asegurando la permanencia, autenticidad y acceso al patrimonio documental digital de Bogotá, hoy y en el futuro.

PARTE INTEGRAL DEL ANEXO TÉCNICO

[17] Ver glosario en 3.4.2 Directrices técnicas y normativas

[18] Ver referentes internacionales y nacionales en 3.4.2 Directrices técnicas y normativas

II. CONTEXTO ESTRATÉGICO DE LAS DIRECTRICES

2.1 Contexto institucional

El Archivo General de Bogotá (AGB), como entidad responsable de orientar la gestión, custodia y preservación del patrimonio documental del Distrito Capital, debe garantizar que la información producida en la administración distrital se mantenga íntegra, auténtica y disponible a lo largo del tiempo. El incremento sostenido de documentos electrónicos, la multiplicidad de sistemas de información utilizados por las entidades y la necesidad de brindar servicios de acceso confiables han hecho evidente la urgencia de contar con una infraestructura especializada que responda a los retos actuales de preservación digital.

En este escenario, la puesta en marcha de un repositorio digital confiable deja de ser una iniciativa aislada para convertirse en un componente estructural de la misión institucional del Archivo General de Bogotá y de la estrategia distrital para la protección y difusión de la memoria documental. La preservación digital, concebida como una función esencial en el ciclo de vida documental, exige condiciones técnicas verificables, procedimientos homogéneos y una arquitectura capaz de sostener el volumen, la complejidad y la diversidad de objetos digitales que alberga el Distrito.

El avance de las políticas de Gobierno Digital, sumado a la creciente demanda ciudadana de transparencia y acceso oportuno a la información pública, ha consolidado un entorno propicio para modernizar los procesos de gestión documental. Este marco normativo se articula directamente con lo dispuesto en la Ley 594 de 2000, el Acuerdo AGN 001 de 2024 y las directrices técnicas del Archivo General de la Nación, que establecen la obligación de asegurar la preservación a largo plazo de los documentos electrónicos, su trazabilidad, valor probatorio y adecuada administración durante todo su ciclo de vida. En este contexto, el Archivo General de Bogotá asume el compromiso de fortalecer su infraestructura tecnológica con criterios de sostenibilidad, interoperabilidad y seguridad.

La formulación del Modelo de Requisitos Funcionales y No Funcionales para la Implementación del Repositorio Archivístico Digital Confiable del Archivo General de Bogotá (AGB) se configura como una herramienta estratégica para orientar el diseño, selección, operación y evaluación de las soluciones tecnológicas que integrarán el ecosistema de preservación digital. Este modelo establece parámetros claros para evitar la adopción de soluciones fragmentadas, garantizar la compatibilidad con los instrumentos archivísticos institucionales incluyendo el Programa de Gestión Documental (PGD), los esquemas de metadatos institucionales y asegurar que las decisiones técnicas respondan a criterios verificables y auditables.

El Archivo General de Bogotá adopta como marco central el Modelo de Referencia OAIS (NTC-ISO 14721[19]), el cual define las funciones esenciales que debe cumplir un repositorio confiable: Ingesta, Almacenamiento Seguro, Gestión de Datos, Administración, Planificación de la Preservación y Acceso. Este enfoque permite estructurar adecuadamente los paquetes de información de transferencia, de archivo y de consulta (PIT, PIA y PIC), fortalecer la cadena de custodia digital y asegurar el uso coherente de metadatos descriptivos, estructurales y de preservación mediante estándares como PREMIS, METS y Dublin Core.

[19] Ver referentes internacionales y nacionales en 3.4.2 Directrices técnicas y normativas

PARTE INTEGRAL DEL ANEXO TÉCNICO

Paralelamente, el modelo incorpora los criterios de la NTC-ISO 16363[20], orientados a la certificación de repositorios digitales confiables. Este estándar aporta lineamientos sobre gobernanza institucional, análisis y mitigación de riesgos tecnológicos, controles de seguridad, disponibilidad operativa, continuidad del servicio y mecanismos de verificación de integridad. Su integración fortalece la capacidad institucional para enfrentar riesgos derivados de la obsolescencia de formatos, fallas de almacenamiento, corrupción de archivos o pérdida de trazabilidad.

El alcance del Archivo General de Bogotá trasciende la definición de requisitos técnicos. Su propósito es consolidar un ecosistema articulado en el cual converjan los procesos archivísticos, la infraestructura tecnológica, la gestión de seguridad de la información y la planeación institucional. Este enfoque integral facilita la interoperabilidad con plataformas distritales, soporta la preparación para transferencias digitales primarias y secundarias, y mejora la capacidad del Archivo General de Bogotá para atender las necesidades de la ciudadanía, las entidades y la comunidad designada.

Además, el modelo sienta las bases para avanzar hacia la implementación plena de un Repositorio Archivístico Digital Confiable, alineado con estándares internacionales y adaptado a las particularidades operativas del Distrito Capital. La aplicación del Archivo General de Bogotá permitirá contar con lineamientos claros para el aseguramiento de la autenticidad, integridad y disponibilidad de los documentos electrónicos, asegurar la sostenibilidad financiera y tecnológica del repositorio, y organizar de manera uniforme los flujos de preservación y acceso.

Con la adopción de este modelo, el Archivo General de Bogotá consolida un paso decisivo hacia una arquitectura de preservación digital moderna, escalable y sostenible. Esta apuesta institucional refleja un compromiso claro con la protección del patrimonio documental, la garantía del acceso público a largo plazo y el fortalecimiento de las funciones esenciales del Estado distrital. En última instancia, este esfuerzo permite asegurar que la memoria documental de Bogotá permanezca viva, íntegra y accesible para las generaciones presentes y futuras.

2.2 Marco normativo y de política pública

Para la consulta el Marco normativo y de política pública, remítase al documento 3.4.2 – Directrices Técnicas y Normativas, en el cual se encuentran definidos los estándares y lineamientos técnicos aplicables a la arquitectura tecnológica del proyecto.

2.3 Articulación institucional y tecnológica

El diseño del Modelo de Requisitos Tecnológicos para la preservación digital del Archivo General de Bogotá (AGB) parte de la necesidad de consolidar una arquitectura capaz de responder al volumen, heterogeneidad y condiciones técnicas identificadas en el diagnóstico de fondos y colecciones documentales digitales. Los resultados del análisis, particularmente la dispersión en nomenclaturas, la multiplicidad de formatos, los vacíos en metadatos y la ausencia de correspondencia sistemática entre estructuras de archivo y jerarquías archivísticas evidencian la urgencia de un modelo que articule, de manera coherente, las funciones archivísticas, los lineamientos institucionales y las capacidades tecnológicas requeridas para un repositorio confiable.

[20] Ver referentes internacionales y nacionales en 3.4.2 Directrices técnicas y normativas

PARTE INTEGRAL DE ANEXO TÉCNICO

El modelo reconoce que la sostenibilidad del repositorio depende de una articulación institucional sólida. En el ámbito interno, esta articulación integra las competencias del equipo de gestión documental, el cual aporta los criterios de organización, valoración y descripción; la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC), responsable de la infraestructura, conectividad, administración de servidores, seguridad perimetral y mecanismos de respaldo; el equipo de seguridad de la información, encargado de los controles, la gestión de riesgos y la protección de datos; y el equipo de preservación digital, que define los parámetros para garantizar integridad, autenticidad y disponibilidad a largo plazo. Esta coordinación es fundamental para que las decisiones técnicas respondan a los requerimientos archivísticos identificados y para que los flujos PIT–PIA–PIC del repositorio reflejen la lógica del fondo, la serie y la unidad documental.

De igual forma, el modelo exige una arquitectura que interactúe con los sistemas distritales que participan en la producción, tramitación, archivo y transferencia de documentos electrónicos. En este sentido, los sistemas de radicación, los servicios de firma digital y electrónica, los módulos de autenticación institucional, los catálogos de metadatos y las plataformas de gestión administrativa deben integrarse con el repositorio bajo criterios comunes de interoperabilidad. Esta integración garantiza que los documentos ingresen al Archivo General de Bogotá con la estructura, completitud de metadatos, formatos, condiciones de acceso y controles de integridad requeridos, evitando reprocesos y asegurando que las transferencias secundarias se ejecuten con trazabilidad y uniformidad en todo el Distrito.

El diagnóstico detallado de fondos y colecciones realizado por el proyecto que incluye la identificación de 1,450,812 archivos, predominancia de imágenes TIFF (77,75 %), presencia de formatos propietarios, archivos sin extensión y registros con metadatos incompletos refuerza la necesidad de un modelo de requisitos que establezca criterios estrictos de validación, normalización, control de integridad y vigilancia tecnológica. Estos criterios deben orientar las decisiones sobre migración, transformación, encapsulación METS, registro de eventos PREMIS y mecanismos de verificación de integridad, conforme a los estándares OAIS, NTC-ISO 16363[21] y a los lineamientos del Acuerdo AGN 001 de 2024.

Para garantizar la coherencia de la arquitectura, el modelo contempla mecanismos formales de coordinación interinstitucional, tales como mesas técnicas, protocolos de interoperabilidad, acuerdos de metadatos, matrices de validación, lineamientos para estrategias de respaldo y procedimientos de revisión archivística y tecnológica. Estos instrumentos permiten que las configuraciones del repositorio, las reglas de ingesta, los parámetros de almacenamiento seguro y los servicios de acceso respondan a una visión institucional común y no a decisiones aisladas. Así mismo, facilitan la incorporación progresiva de nuevas entidades del Distrito, asegurando que los sistemas de gestión se integren al repositorio bajo reglas interoperables y sostenibles.

El modelo también reconoce que la preservación digital es un proceso en evolución permanente. En consecuencia, establece la necesidad de revisar y actualizar periódicamente los requisitos tecnológicos, considerando la evolución normativa, las transformaciones en infraestructura, la obsolescencia de los formatos y los resultados del monitoreo continuo del repositorio. La capacitación del personal, la adopción de metodologías de aseguramiento de la calidad y el seguimiento de estándares

[21] Ver referentes internacionales y nacionales en 3.4.2 Directrices técnicas y normativas

PARTE INTEGRAL DE ANEXO 5 CNSC

internacionales complementan este proceso, fortaleciendo la capacidad operativa y analítica del Archivo General de Bogotá.

Como resultado, el Modelo de Requisitos Tecnológicos configura una arquitectura integral y coherente, donde los procesos archivísticos, los sistemas de información, los estándares técnicos y la infraestructura de preservación operan como un sistema único y articulado. Esta visión permite al Archivo General de Bogotá avanzar hacia un repositorio digital seguro, auditable, interoperable y sostenible, capaz de garantizar la preservación de la memoria documental del Distrito Capital y de soportar, con solidez técnica, la gestión documental del futuro.

PARTE INTEGRAL DEL ANEXO TÉCNICO

III. ENFOQUE Y METODOLOGÍA

3.1 Enfoque general

El modelo de arquitectura conceptual y tecnológica que orienta el proyecto de preservación digital del Archivo General de Bogotá se fundamenta en un enfoque de fortalecimiento institucional progresivo, que articula la capacidad técnica instalada con las necesidades reales identificadas durante el diagnóstico distrital de fondos y colecciones digitales. Este enfoque reconoce que la preservación digital es un proceso de madurez gradual y continuo, que exige coherencia entre las funciones archivísticas, las políticas institucionales, la infraestructura tecnológica y la gestión de riesgos.

El modelo integra dos referentes metodológicos clave. Por un lado, el Sistema Integrado de Conservación (SIC) de la Secretaria General de la Alcaldía Mayor de Bogotá, que define las responsabilidades institucionales en materia de conservación, preservación, gestión del riesgo y continuidad operativa del patrimonio documental. Por otro, los NDSA Levels of Digital Preservation (v2, 2022), que permiten evaluar y proyectar el nivel de madurez alcanzado en dimensiones como almacenamiento, integridad, control de metadatos, planeación de preservación y acceso seguro. Así mismos el modelo TOGAF[22] para la definición de la arquitectura tecnológica que utiliza para su completitud estrategias de la Guía para requemamientos ISO/IEC TR 24766:2009[23] y el modelado UML[24], ajustadas para el Archivo General de Bogotá.

La combinación de los tres (3) marcos ofrece una visión clara de los avances, brechas y acciones prioritarias que deben implementarse para consolidar un repositorio archivístico digital confiable y sostenible en el tiempo.

A partir de este marco combinado, se desarrolló un diagnóstico exhaustivo del estado de la preservación digital en el Distrito, sustentado en el análisis técnico de los objetos digitales transferidos y en la revisión de capacidades institucionales. Este diagnóstico incluyó la caracterización masiva de formatos, la identificación de archivos corruptos o incompletos, la verificación de metadatos técnicos y descriptivos, el análisis de riesgos de obsolescencia, la evaluación del almacenamiento disponible, y la revisión de la integridad mediante controles de hash. Estos insumos permitieron definir una línea base realista y priorizar las decisiones que componen la arquitectura tecnológica del repositorio digital.

El enfoque por niveles plantea un desarrollo gradual y ordenado. En sus primeras fases, se concentra en el fortalecimiento de capacidades esenciales, tales como la organización y depuración de estructuras de archivos, la estandarización de nomenclaturas, la normalización de metadatos y la definición de flujos consistentes para las transferencias documentales. Posteriormente, se avanza hacia escenarios de preservación activa, que incluyen la automatización de controles de integridad, la generación de paquetes de preservación basados en OAIS (SIP, AIP, DIP), la verificación periódica de fixity, el monitoreo de obsolescencia tecnológica y la implementación de mecanismos de redundancia y recuperación ante desastres. En fases avanzadas, se incorporan prácticas que permiten aspirar a procesos de auditoría

[22] Ver glosario en 3.4.2 Directrices técnicas y normativas

[23] Ver referentes internacionales y nacionales en 3.4.2 Directrices técnicas y normativas

[24] Ver tabla de acrónimos

externa o certificación conforme a la NTC-ISO 16363[25], fortaleciendo la confiabilidad institucional del repositorio.

La hoja de ruta resultante facilita la adopción progresiva de estándares internacionales y buenas prácticas, entre ellas:

- el uso sistemático de formatos abiertos y documentados;
- la construcción y mantenimiento de metadatos de preservación (PREMIS), empaquetamiento (METS) y descripción (Dublin Core e ISAD(G));
- la documentación formal de procesos archivísticos, tecnológicos y de preservación;
- la gestión permanente del riesgo tecnológico y operativo;
- la verificación continua de integridad mediante algoritmos robustos de hash;
- y la adopción de protocolos homogéneos para las transferencias primarias, secundarias y electrónicas provenientes de las entidades distritales.

Este conjunto de lineamientos garantiza que la arquitectura diseñada responda a criterios de realismo operativo, escalabilidad, sostenibilidad financiera y adecuación tecnológica. Además, permite armonizar las decisiones del proyecto con los sistemas institucionales existentes, con los flujos documentales propios del Distrito y con los instrumentos archivísticos del Archivo General de Bogotá incluidas las TRD/TVD, el Programa de Gestión Documental y el Esquema Institucional de Metadatos.

En síntesis, el Modelo de Requisitos Tecnológicos constituye la base estructural para avanzar hacia un Repositorio Digital de Confianza, preparado para adaptarse a los cambios tecnológicos, cumplir de manera estricta con la normativa archivística vigente y garantizar la autenticidad, integridad, trazabilidad y disponibilidad del patrimonio documental digital de Bogotá. Con esta apuesta, el Archivo General de Bogotá consolida una arquitectura moderna, auditable y sostenible, acorde con su misión de custodiar y preservar la memoria documental del Distrito Capital para las generaciones futuras.

3.2 Estructura metodológica

La metodología empleada para el diseño del modelo de requisitos asociado al proyecto de preservación digital del Archivo General de Bogotá se estructuró en un proceso gradual, riguroso y orientado a garantizar coherencia técnica, normativa y operativa. Su objetivo principal fue asegurar que los requisitos tecnológicos definidos respondieran a la realidad institucional, a la caracterización de los fondos y colecciones digitales y a las necesidades de preservación a largo plazo evidenciadas en el diagnóstico general del proyecto.

Este proceso metodológico se desarrolló en cinco fases integradas, cada una aportando insumos fundamentales para construir un modelo robusto, verificable y alineado con los estándares internacionales y la normatividad archivística vigente.

1. Diagnóstico técnico integral

[25] Ver referentes internacionales y nacionales en 3.4.2 Directrices técnicas y normativas

COPIA INTEGRA DEL ANEXO TECNICO

La primera fase consistió en una revisión exhaustiva de los diagnósticos previos entregables 3.2.1, 3.2.2 y 3.2.3 junto con los resultados del análisis técnico de fondos y colecciones documentales digitales.

Esta revisión permitió:

- Identificar el estado real de los objetos digitales custodios del AGB[26].
- Caracterizar formatos, extensiones, tamaños, riesgos y obsolescencias.
- Verificar niveles de integridad, duplicidad y consistencia de metadatos.
- Analizar la estructura de almacenamiento, nomenclaturas y rutas de acceso.
- Reconocer vacíos, inconsistencias y oportunidades de mejora en los procesos de preservación.

Gracias a esta fase, se obtuvieron parámetros claros para orientar el diseño del ecosistema tecnológico, especialmente en temas de interoperabilidad, estandarización de metadatos, mecanismos de control de integridad y requisitos de infraestructura.

2. Diseño del marco de directrices

En esta fase se consolidaron los lineamientos técnicos y normativos que enmarcan la arquitectura del repositorio digital. Se realizó un análisis comparativo y aplicado de:

- NTC-ISO 14721[27] – OAIS, como eje para la definición de funciones, flujos SIP–AIP–DIP y entidades de administración, acceso y almacenamiento.
- NTC-ISO 16363[28], para incorporar criterios de auditoría, gobernanza, sostenibilidad y confiabilidad.
- NTC-ISO 15489[29] y NTC-ISO 30301[30], referentes para los sistemas de gestión documental.
- Acuerdo AGN 001 de 2024, como base para la producción, gestión, transferencia y preservación digital de los documentos electrónicos de archivo.
- CONPES 3975 y 3995, aplicables al fortalecimiento de la memoria histórica y la transformación digital.
- Política de Gobierno Digital y normativa distrital aplicable (Decreto 828 de 2018, Decreto 1008 de 2018, entre otros).
- Modelo TOGAF[31],
- Guía para requemamientos ISO/IEC TR 24766:2009[32] y

[26] Ver tabla de acrónimos
[27] Ver referentes internacionales y nacionales en 3.4.2 Directrices técnicas y normativas
[28] Ver referentes internacionales y nacionales en 3.4.2 Directrices técnicas y normativas
[29] Ver referentes internacionales y nacionales en 3.4.2 Directrices técnicas y normativas
[30] Ver referentes internacionales y nacionales en 3.4.2 Directrices técnicas y normativas
[31] Ver tabla de acrónimos
[32] Ver referentes internacionales y nacionales en 3.4.2 Directrices técnicas y normativas

PARTE INTEGRAL DEL ANEXO TÉCNICO

- el modelado UML[33]

Este ejercicio generó un cuerpo de directrices normativo–técnicas que fundamenta los requisitos del sistema, alineando los elementos archivísticos, tecnológicos y de preservación.

3. Definición de matrices de aplicabilidad normativa

Como herramienta operativa, se elaboraron matrices que relacionan cada área del modelo con las normas aplicables, detallando:

- obligaciones institucionales,
- criterios verificables de cumplimiento,
- tipos de evidencia requeridos,
- periodicidad de revisión y auditoría,
- riesgos asociados al incumplimiento.

Estas matrices se convierten en un instrumento de control esencial para la implementación del repositorio, permitiendo una trazabilidad verificable y facilitando procesos de auditoría interna y externa en materia de preservación digital.

4. Articulación con los demás componentes de la arquitectura tecnológica

Esta fase buscó integrar coherentemente el Modelo de Requisitos Tecnológicos con:

- el Modelo de Arquitectura Conceptual y Tecnológica (3.4.3),
- las Especificaciones Técnicas de Hardware y Software (3.4.4),
- el análisis de riesgos técnicos y archivísticos,
- los resultados del diagnóstico de entidades distritales (3.3).

La articulación permitió garantizar:

- consistencia entre decisiones estratégicas, técnicas y operativas;
- compatibilidad entre los componentes tecnológicos del ecosistema del Archivo General de Bogotá;
- alineación entre procesos archivísticos, estructura tecnológica y políticas institucionales;
- definición de flujos integrados de ingesta, almacenamiento, acceso y preservación;
- coherencia entre infraestructura física, lógica y objetivos de preservación.

PARTE INTEGRAL DEL ANEXO TÉCNICO

[33] Ver tabla de acrónimos

5. Armonización con el Plan General del Proyecto de Diagnóstico

Finalmente, se realizó un ejercicio de alineación entre las directrices formuladas y los objetivos del Plan General del Proyecto, con el fin de asegurar que:

- las propuestas respondan a las necesidades reales del Archivo General de Bogotá;
- exista coherencia entre la arquitectura tecnológica y las políticas distritales sobre memoria, acceso y preservación;
- los requisitos tecnológicos fortalezcan la gestión y la sostenibilidad del patrimonio documental digital del Distrito;
- la ruta metodológica establecida pueda ser implementada en fases realistas y verificables.

Este proceso de armonización permitió integrar los resultados del diagnóstico, la arquitectura planteada y la visión estratégica institucional, consolidando las bases del futuro Repositorio Archivístico Digital confiable del Distrito Capital.

La metodología adoptada para el diseño del Modelo de Requisitos Tecnológicos permitió construir una propuesta sólida, coherente con la realidad técnica del Archivo General de Bogotá y sustentada en estándares internacionales. Su carácter gradual y su enfoque integral garantizan que la arquitectura resultante sea viable, escalable y sostenible, permitiendo avanzar de manera ordenada hacia un ecosistema de preservación digital robusto, confiable y articulado con las funciones misionales del Archivo General de Bogotá.

PARTE INTEGRAL DEL ANEXO TÉCNICO

IV. MODELO DE REQUISITOS TECNOLÓGICOS

4.1 Objetivo del Modelo de Requisitos Archivo General de Bogotá.

Definir los requisitos funcionales y no funcionales necesarios para la implementación de un repositorio digital confiable en el Archivo General de Bogotá, con el fin de asegurar la autenticidad, integridad, confidencialidad, disponibilidad, accesibilidad e interoperabilidad de los documentos electrónicos de archivo, garantizando su conservación a largo plazo y fortaleciendo el cumplimiento de la función misional de la entidad.

4.2 Alcance

Los requisitos aquí consignados aplican a los objetos digitales de carácter archivístico bajo custodia del Archivo General de Bogotá que hacen parte de los fondos documentales definidos en el marco del proyecto, en particular aquellos que ingresan al repositorio a través de los flujos de transferencia PIT–PIA–PIC, conforme a los lineamientos establecidos para las transferencias electrónicas secundarias.

En este sentido, el alcance no se extiende de manera indiscriminada a cualquier objeto digital, sino que se circunscribe a los Documentos Electrónicos de Archivo (DEA) y a los objetos digitales derivados de procesos de digitalización, valoración, descripción y preservación que han sido formalmente transferidos o se encuentran en proceso de transferencia al Archivo General de Bogotá, de acuerdo con las Tablas de Retención y Valoración Documental vigentes y el Protocolo de Transferencias descrito en el numeral

Los requisitos deberán incorporarse de manera progresiva en los procedimientos técnicos, tecnológicos y archivísticos definidos para la operación del Repositorio Archivístico Digital Confiable del AGB, el cual tiene como finalidad principal garantizar el almacenamiento archivístico seguro, confiable y sostenible de los objetos digitales bajo su custodia, asegurando la autenticidad, integridad, trazabilidad y disponibilidad a largo plazo.

El repositorio estará orientado por los principios archivísticos de procedencia y orden original, permitiendo la correcta organización de los fondos, secciones, series, subseries, expedientes y tipos documentales, y deberá integrar mecanismos que faciliten la interoperabilidad con los Sistemas de Gestión de Documentos Electrónicos de Archivo (SGDEA) y demás plataformas de información del Distrito Capital, sin sustituir sus funciones misionales, sino actuando como infraestructura de preservación y custodia definitiva.

Los requisitos definidos se enmarcan en el Sistema Distrital de Archivos (SDA) y tienen como propósito fortalecer las capacidades del Archivo General de Bogotá para ejercer su rol como ente rector del SDA, así como brindar soporte técnico y archivístico a las entidades distritales en los procesos de transferencia electrónica secundaria, asegurando condiciones homogéneas, verificables y alineadas con el modelo OAIS (ISO 14721), la Ley 594 de 2000 y el Acuerdo 001 de 2024 del AGN.

Consideraciones generales para un Repositorio Archivístico Digital Confiable

1. Responsabilidad institucional

   El diseño, implementación, administración y monitoreo del repositorio deberán ser responsabilidad del Archivo General de Bogotá, mediante equipos

PARA INTEGRACIÓN AL PETH

multidisciplinarios conformados por archivistas, ingenieros de sistemas y especialistas en preservación digital. Esta articulación garantiza un enfoque integral que combine la normativa archivística, la arquitectura tecnológica y las estrategias de preservación a largo plazo, en concordancia con los roles definidos en el SDA.

2. Clasificación y organización documental

   El repositorio deberá soportar la organización jerárquica de los documentos conforme al Cuadro de Clasificación Documental, permitiendo la conformación y gestión de expedientes electrónicos, así como la descripción multinivel de fondos y colecciones digitales. Esta estructura es condición indispensable para la recuperación de la información, el control archivístico y la correcta interpretación del contexto de producción.

3. Preservación digital continua

   Desde la admisión de los objetos digitales (SIP), el repositorio deberá aplicar estrategias activas de preservación digital, incluyendo controles de integridad (hash), registro de eventos de preservación y transformaciones, y gestión de metadatos de procedencia, contexto y derechos, con énfasis en esquemas como PREMIS y METS. Estas acciones deben garantizar la autenticidad y confiabilidad de los documentos, incluso en escenarios de migración tecnológica o de formatos.

4. Independencia tecnológica

   El repositorio deberá asegurar el acceso controlado y la preservación de los documentos sin depender de aplicaciones propietarias o externas que comprometan la sostenibilidad del sistema. La arquitectura deberá minimizar riesgos asociados a la obsolescencia tecnológica, privilegiando estándares abiertos y mecanismos que permitan la evolución controlada de la plataforma.

5. Interoperabilidad y estándares

   El sistema deberá interoperar con otros repositorios y plataformas de gestión documental del Distrito, respetando estándares nacionales e internacionales en materia archivística y tecnológica. Esta interoperabilidad es clave para soportar los flujos de transferencia electrónica, la consulta controlada y la articulación con los SGDEA de las entidades productoras.

6. Continuidad del servicio

   El repositorio deberá contar con planes de contingencia, respaldo y recuperación ante incidentes, desastres naturales o fallas tecnológicas, alineados con las directrices de la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) y los planes de continuidad institucional del Archivo General de Bogotá. Estos mecanismos deben garantizar la disponibilidad y protección del patrimonio documental digital bajo custodia.

4.3 Requisitos Funcionales

Los requisitos funcionales del Repositorio Archivístico Digital Confiable se estructuran conforme a las funciones y procesos establecidos en el Modelo de Referencia OAIS,

PARTE INTEGRAL DEL ANEXO TÉCNICO

integrando criterios archivísticos, tecnológicos y de preservación que garantizan el cumplimiento de la misión institucional del Archivo General de Bogotá (AGB). Dichos requisitos responden a la necesidad de disponer de un sistema confiable capaz de gestionar, preservar y poner a disposición el patrimonio documental digital del Distrito Capital bajo condiciones que aseguren su integridad, autenticidad y disponibilidad en el tiempo.

El Repositorio Archivístico Digital Confiables incluye el capacidades especificas para el tratamiento en todas las etapas (Ingesta, Archivo y Consulta) de los fondos documentales históricos con los que cuenta el Archivo General de Bogotá.

Para cumplir estos propósitos, el sistema deberá incorporar capacidades que garanticen:

1. **Ingesta controlada y verificable de documentos electrónicos.**

El repositorio debe permitir la recepción estructurada de paquetes de información de transferencia (PIT) provenientes de entidades productoras, asegurando la validación automática de formatos, consistencia de metadatos, integridad mediante algoritmos de hash y correspondencia con los instrumentos archivísticos del Archivo General de Bogotá. La ingesta deberá registrar eventos, productores, fechas, controles de calidad y resultados de verificación para mantener trazabilidad completa del proceso.

2. **Almacenamiento seguro, redundante y orientado a preservación.**

El repositorio deberá implementar mecanismos que garanticen la conservación íntegra de los objetos digitales:

- replicación geográfica,
- almacenamiento inmutable cuando aplique,
- estrategias de respaldo 3-2-1,
- monitoreo de hardware,
- validación periódica de integridad y
- herramientas para detectar corrupción silenciosa de datos.
- El Repositorio Archivístico Digital Confiable debe permitir la administración de Paquetes de Información de Archivo con metadatos PREMIS completos sobre eventos, agentes, derechos y características técnicas.

3**. Gestión archivística y administración de metadatos.**

Los requisitos contemplan la administración de metadatos descriptivos, técnicos, estructurales y de preservación, con soporte para esquemas como ISAD(G)[34], Dublin Core[35], METS[36] y PREMIS[37]. La plataforma deberá facilitar la vinculación entre estructuras archivísticas (fondo, sección, serie, subserie, expediente) y los objetos digitales, garantizando coherencia entre la descripción archivística y los paquetes de preservación.

4. **Planificación de la preservación y gestión del riesgo tecnológico.**

[34] Ver glosario en 3.4.2 Directrices técnicas y normativas
[35] Ver glosario en 3.4.2 Directrices técnicas y normativas
[36] Ver glosario en 3.4.2 Directrices técnicas y normativas
[37] Ver glosario en 3.4.2 Directrices técnicas y normativas

PARTE INTEGRAL DEL ANEXO TÉCNICO

Deberá permitir la identificación y tratamiento de riesgos de obsolescencia mediante esquemas de vigilancia tecnológica, control de formatos, políticas de migración y registro de acciones de preservación. Esto incluye contar con herramientas para evaluar formatos, detectar riesgos, planear intervenciones y documentar decisiones en concordancia con los lineamientos del Archivo General de Bogotá y los criterios definidos en el diagnóstico técnico de formatos y metadatos.

5. **Acceso seguro, controlado e interoperable.**

El repositorio deberá generar Paquetes de Información de Consulta (PIC) en condiciones de acceso acordes con la normativa vigente (Ley 1712 de 2014, protección de datos personales, restricciones por derechos de autor). Asimismo, debe ofrecer mecanismos de consulta y descarga controlada, garantizar integridad en la entrega de información y articularse con sistemas distritales a través de APIs, metadatos interoperables y estructuras estandarizadas de intercambio digital.

La adopción de estos requisitos funcionales permite asegurar que el Repositorio Archivístico Digital Confiable del Archivo General de Bogotá opere bajo condiciones que responden a los estándares internacionales de preservación digital NTC-ISO 14721[38] (OAIS) y NTC-ISO 16363[39], y se articule plenamente con las directrices del Archivo General de la Nación y del Sistema Distrital de Archivos. Con ello, se establecen las bases técnicas y archivísticas para un sistema confiable, auditable y preparado para enfrentar los desafíos presentes y futuros de la preservación del patrimonio documental digital de la ciudad.

R1. Estructura del paquete de información

Con el fin de asegurar la organización, trazabilidad y preservación a largo plazo de los objetos digitales que ingresan al Archivo General de Bogotá (AGB), se definen los siguientes requisitos técnicos para la conformación y estructuración de los paquetes de información. Estos lineamientos permiten uniformar los procedimientos de ingesta, facilitar la interoperabilidad con sistemas distritales, garantizar la integridad de los objetos digitales y asegurar que los procesos de almacenamiento y preservación se ajusten a los estándares internacionales adoptados por la institución.

Los requisitos se fundamentan en las necesidades identificadas en el diagnóstico técnico de fondos y colecciones digitales, en las buenas prácticas establecidas por los modelos OAIS[40], PREMIS[41] y METS[42], y en los criterios de organización requeridos para mantener un control archivístico confiable.

R1.1. El sistema debe organizar cada Paquete de Información de Transferencia (PIT)[43] en una única carpeta lógica. En el nivel superior no debe existir más de una carpeta, para garantizar la unidad intelectual del PI y evitar ambigüedades en la administración de los objetos digitales.

COPIA INTEGRAL DEL ANEXO TÉCNICO

[38] Ver referentes internacionales y nacionales en 3.4.2 Directrices técnicas y normativas
[39] Ver referentes internacionales y nacionales en 3.4.2 Directrices técnicas y normativas
[40] Ver glosario en 3.4.2 Directrices técnicas y normativas
[41] Ver glosario en 3.4.2 Directrices técnicas y normativas
[42] Ver glosario en 3.4.2 Directrices técnicas y normativas
[43] Ver glosario en 3.4.2 Directrices técnicas y normativas

R1.2. La carpeta principal debe identificarse mediante un identificador único persistente, preferiblemente bajo un estándar UUID[44]. Esto asegura unicidad, facilita el seguimiento de los eventos de preservación y mantiene coherencia con los mecanismos de trazabilidad definidos por el Archivo General de Bogotá.

R1.3. El sistema debe permitir la compresión de los Paquetes de Información de Transferencia (PIT)[45] en formatos aceptados para preservación y transferencia (TAR[46] o ZIP[47] sin pérdida), manteniendo la integridad de la estructura interna del paquete.

R1.4. Cada Paquete de Información PIT[48] debe incluir en su nivel superior un archivo METS.xml, que documente la identidad, estructura, relaciones internas y vínculos con los esquemas de metadatos utilizados. Este archivo constituye el punto central de descripción estructural y funcional del paquete.

R1.5. El Paquetes de Información PI debe contar con una carpeta denominada “metadatos”, en la cual se almacenen los metadatos relevantes para su gestión, preservación y recuperación.

R1.6. Los metadatos de preservación (PREMIS) deben alojarse en subcarpetas específicas dentro de la carpeta “metadatos”, permitiendo registrar eventos, agentes, derechos y acciones técnicas necesarias para asegurar preservación a largo plazo.

R1.7. Los metadatos descriptivos deben organizarse en subcarpetas propias dentro de la carpeta “metadatos”, asegurando su independencia respecto a los elementos técnicos y preservación.

R1.8. Otros tipos de metadatos (contextuales, técnicos ampliados, informes complementarios, etc.) podrán organizarse en subcarpetas adicionales, por ejemplo, “otros” siempre que conserven una estructura clara y documentada.

R1.9. El Paquete de Información PI debe incluir una carpeta “representaciones”, destinada a consolidar las diferentes versiones o representaciones digitales de los documentos que lo componen.

R1.10. Cada representación debe ubicarse dentro de una subcarpeta independiente, con un nombre único y verificable, permitiendo diferenciar versiones, copias maestras, derivados o subproductos.

R1.11. En cada representación debe existir una subcarpeta “datos”, destinada exclusivamente a los archivos digitales que conforman dicha representación.

R1.12. Cada representación podrá incluir su propio archivo METS.xml, cuando se requiera documentar estructuras internas, dependencias técnicas o metadatos propios de esa versión.

R1.13. Si existe metadato adicional para una representación específica, debe organizarse en una subcarpeta “metadatos” dentro de la representación, manteniendo la separación lógica establecida.

PARTE INTEGRAL DEL ANEXO TÉCNICO

[44] Ver glosario en 3.4.2 Directrices técnicas y normativas
[45] Ver glosario en 3.4.2 Directrices técnicas y normativas
[46] Ver glosario en 3.4.2 Directrices técnicas y normativas
[47] Ver glosario en 3.4.2 Directrices técnicas y normativas
[48] Ver glosario en 3.4.2 Directrices técnicas y normativas

R1.14. Tanto el paquete como las representaciones pueden incluir subcarpetas adicionales, siempre que exista justificación técnica o archivística, y que dichas carpetas no alteren la estructura mínima definida.

R1.15. Los esquemas XML[49] necesarios para la validación de los paquetes deben ubicarse en una subcarpeta denominada “esquemas”, facilitando verificaciones internas y asegurando el control de versiones.

R1.16. La documentación complementaria, tales como actas, informes, notas técnicas, referencias externas o documentos que contextualicen el contenido del paquete de Información (PI) debe organizarse en una subcarpeta llamada “documentación”.

R1.17. Los implementadores podrán agregar carpetas o estructuras adicionales cuando las necesidades del proceso, del fondo o del tipo documental lo requieran, siempre que se preserve la estructura básica y se documente cualquier ampliación realizada.

R1.18. El sistema deberá garantizar que todos los Paquetes de Información (SIP, PIA y PIC) cuenten con una estructura normalizada, verificable y autoexplicativa, que permita su interpretación independiente a largo plazo. Cada paquete deberá integrar de manera coherente los objetos digitales, los metadatos descriptivos, técnicos, administrativos y de preservación, así como la documentación asociada a su contexto de producción y custodia.

R1.19.Se deberá asegurar la incorporación de identificadores persistentes bajo políticas de nombres globales (namespace institucional + UUID), evitando colisiones y facilitando la interoperabilidad con otros repositorios OAIS. La estructura del paquete deberá soportar METS como mecanismo de empaquetamiento, con referencias explícitas a metadatos PREMIS, Dublin Core y, cuando aplique, EAD.

R1.20.El sistema deberá preservar la red de representación, incluyendo información semántica, estructural y técnica que permita comprender y reutilizar los objetos digitales sin depender de sistemas externos.

Estos requisitos permiten estandarizar la ingesta de documentos digitales, corregir las inconsistencias evidenciadas en el diagnóstico (duplicidad, ausencia de metadatos, falta de correspondencia entre estructuras de almacenamiento e instrumentos archivísticos) y establecer una base sólida para la construcción del Repositorio Archivístico Digital Confiable del Archivo General de Bogotá.

R2. Requisitos para la admisión

La admisión corresponde al momento en el cual los documentos electrónicos y sus metadatos asociados ingresan formalmente al repositorio digital del Archivo General de Bogotá. En esta etapa, el paquete de información de Transferencia (PIT) es sometido a un conjunto de verificaciones, validaciones y registros que permiten transformarlo en un Paquete de Información de Archivo (PIA), asegurando que cumpla con las condiciones mínimas para su preservación a largo plazo. Esta fase constituye un punto crítico dentro del modelo OAIS, pues garantiza la autenticidad, integridad y trazabilidad del acervo digital que custodia el Archivo General de Bogotá.

Con base en estos principios, se establecen los siguientes requisitos:

[49] Ver glosario en 3.4.2 Directrices técnicas y normativas

PARTE INTEGRAL DEL ANEXO TÉCNICO

Requisitos para la admisión de Paquetes de Información de Transferencia PIA (Ingreso – Transformación a Paquetes de Información de Archivo), buscando mitigar problemas de interoperabilidad y cumplir con las directrices de normalización estructural definidas en el entregables 3.4.2 Directrices Técnicas y Normativas.

R2.1. Identificación de atributos del documento a conservar. Debe incluir capacidades para permitir identificar y registrar, de manera automática o semiautomática, los atributos esenciales del documento electrónico. Esto incluye contenido, nombre de archivo, formato, resolución, tamaño, duración (en el caso de audiovisuales), número de páginas y cualquier otro elemento técnico indispensable que se agregue en el futuro para garantizar su preservación futura.

R2.2. Nomenclatura de los paquetes. Debe incluir capacidades para rechazar o colocar en cuarentena paquetes de Información de Transferencia (PIT) con errores de nomenclatura critica tales como:

- Espacios en blanco
- Caracteres especiales
- Inconsistencias en mayúsculas y minúsculas

R2.3. Asociación y validación de metadatos durante la presentación del Paquete de Información de Transferencia (PIT). Durante la admisión, el repositorio debe incluir capacidades para permitir vincular metadatos descriptivos, técnicos, administrativos y de preservación. La plataforma debe validar la completitud mínima requerida, detectar inconsistencias y asegurar la correspondencia entre metadatos y documentos.

R2.4. Mecanismos de autenticación de origen. Debe contar con capacidades a nivel de procesos que permitan verificar la legitimidad del productor o entidad que realiza la transferencia. Estos mecanismos pueden ser manuales (certificación archivística) o automáticos (firma digital, certificados de autenticación, comprobación de remitentes institucionales).

R2.5. Verificación de integridad del Paquete de Información de Transferencia (PIT). La admisión debe incluir controles de integridad mediante algoritmos de hash (SHA-128, SHA-256[50] o superior). Debe contar con capacidades para recalcular y comparar los valores de integridad con los entregados en la transferencia, registrando discrepancias y generando alertas cuando corresponda.

R2.6. Control físico de bits. Debe incluir capacidades para ejecutar procedimientos de validación a nivel de bitstream[51], asegurando que los archivos no presenten corrupción, truncamiento, sectores ilegibles o alteraciones que comprometan su preservación. Este control debe quedar documentado en los metadatos de preservación (PREMIS[52]).

R2.7. Generación de informes de progreso. Debe incluir capacidades para emitir reportes detallados sobre el avance del proceso de admisión, indicando etapas completadas, alertas, fallos, tiempos de procesamiento y estadísticas básicas, con el propósito de facilitar los procesos de auditoría, trazabilidad y transparencia durante la ingesta.

PARTE INTEGRAL DEL ANEXO TÉCNICO

[50] Ver glosario en 3.4.2 Directrices técnicas y normativas

[51] Ver glosario en 3.4.2 Directrices técnicas y normativas

[52] Ver glosario en 3.4.2 Directrices técnicas y normativas

R2.8. Notificaciones y reportes de aceptación de responsabilidad de preservación. Una vez finalizada la admisión, debe incluir capacidades para emitir un reporte formal que certifique la aceptación del paquete como Paquete de Información de Archivo (PIA). Este informe constituye el acto archivístico mediante el cual el Archivo General de Bogotá asume la responsabilidad de preservarlo a largo plazo.

R2.9. Registro de acciones archivísticas y tecnológicas en formatos abiertos. Debe incluir capacidades para registrar todas las acciones ejecutadas durante la admisión validaciones, controles, correcciones, reasignaciones, verificaciones de integridad, aplicación de metadatos, en formatos abiertos que permitan auditoría, interoperabilidad y acceso futuro, como por ejemplo XML[53], JSON[54] o CSV[55].

R2.10.El repositorio deberá disponer de un módulo especializado para la creación y admisión de Paquetes de Información de Envío (SIP) listos para OAIS, a partir de archivos y carpetas locales o provenientes de sistemas productores. Este módulo deberá permitir la creación individual y masiva de SIP válidos, soportando miles de paquetes en una sola operación, sin pérdida de rendimiento ni trazabilidad.

R2.10.Durante la admisión se deberán ejecutar validaciones automáticas de estructura, formatos, integridad (hash), correspondencia archivística y completitud de metadatos, registrando los resultados de aceptación o rechazo en pistas de auditoría inalterables. El sistema deberá gestionar formalmente los Submission Agreements, asegurando que cada SIP cumpla las condiciones técnicas y archivísticas previamente acordadas con la entidad transferente.

Estos requisitos fortalecen la calidad del proceso de ingreso, garantizan la confiabilidad del repositorio y permiten que la transformación del Paquete de Información de Transferencia (PIT) a Paquete de Información de Archivo (PIA) se realice bajo criterios verificables, garantizando la autenticidad e inalterabilidad de los objetos digitales de acuerdo con la normatividad nacional en materia de gestión de documentos electrónicos (acuerdo 01 AGN 001 de 2024[56]) y consistentes con los estándares internacionales y con las condiciones técnicas identificadas en los diagnósticos de fondos y colecciones del Archivo General de Bogotá.

R3. Requisitos para la creación de Paquetes de Información de Archivo (PIA)

En el marco de las funciones de Almacenamiento Seguro y Planificación de la Preservación del modelo OAIS, el Repositorio Archivístico Digital Confiable del Archivo General de Bogotá debe contar con mecanismos estructurados para garantizar la disponibilidad, integridad, trazabilidad y conservación de las distintas clases de información que conforman los Paquetes de Información de Archivo (PIA). Para ello, se definen los siguientes requisitos funcionales, orientados a asegurar que cada objeto digital sea administrado con los metadatos, controles y acciones de preservación adecuados.

Requisitos para la gestión, almacenamiento y preservación de los Paquetes de Información de Archivo (PIA).

[53] Ver glosario en 3.4.2 Directrices técnicas y normativas
[54] Ver glosario en 3.4.2 Directrices técnicas y normativas
[55] Ver glosario en 3.4.2 Directrices técnicas y normativas
[56] Ver glosario en 3.4.2 Directrices técnicas y normativas

R3.1. Descripción detallada de cada clase de información. Debe incluir capacidades para permitir identificar y caracterizar cada tipo de contenido (imagen fija, texto, bases de datos, audio, video, registros mixtos), registrando sus atributos técnicos y archivísticos. Esta descripción debe alinearse con la estructura de metadatos definida en los instrumentos institucionales y con los resultados del diagnóstico técnico de formatos realizado por el Archivo General de Bogotá.

R3.2. Soporte a la preservación diferenciada según el tipo de contenido. Debe incluir capacidades para implementar acciones específicas de preservación según la naturaleza del documento, entre las que se incluyen:

- control de resolución y profundidad de bits en imágenes;
- monitoreo de códecs en audiovisuales;
- normalización de estructuras en bases de datos;
- validaciones de PDF/A en documentos textuales;

Estas acciones deben documentarse y ejecutarse de manera sistemática.

R3.3. Documentación completa de las transformaciones realizadas entre el Paquete de información de Transferencia (PIT) y el Paquete de Información de Archivo (PIA). Debe incluir capacidades para que toda modificación, validación o proceso de normalización ejecutado para convertir el PIT y en un PIA incluyendo reorganización de carpetas, incorporación de metadatos, cálculos de integridad o ajustes técnicos debe quedar registrado mediante metadatos de preservación (PREMIS), garantizando trazabilidad total del proceso.

R3.4. Reportes sobre aceptación o rechazo de los Paquetes de Información de Transferencia (PIT) procesados. Debe incluir capacidades para generar informes automatizados que indiquen si un PIT fue aceptado como PIA, rechazado o requiere correcciones. Estos reportes deben detallar causas, errores, alertas y evidencias asociadas, asegurando transparencia y control del proceso de admisión y almacenamiento.

R3.5. Asignación de identificadores UUID[57] únicos y persistentes. Cada Paquete de Información de Transferencia (PIT) y cada representación contenida en él deben contar con un identificador único (UUID) que permita su localización inequívoca, su vinculación con metadatos descriptivos. Este identificador debe mantenerse estable durante todo tiempo que esté en el Repositorio Archivístico Digital Confiable.

R3.6. Integración con herramientas de monitoreo y control de formatos. El repositorio debe integrarse con fuentes de referencia como PRONOM[58], NARA[59] y otros servicios de identificación de formatos, permitiendo la detección oportuna de riesgos de obsolescencia, dependencias técnicas, incompatibilidades y necesidades futuras de migración.

R3.7. Uso de formatos de preservación recomendados. Debe incluir capacidades para la validación automática para que documentos textuales cumplan con el estándar PDF/A (NTC-ISO 19005) y los archivos de imagen cumplen con el TIFF (formato de archivo de

[57] Ver glosario en 3.4.2 Directrices técnicas y normativas

[58] Ver glosario en 3.4.2 Directrices técnicas y normativas

[59] Ver glosario en 3.4.2 Directrices técnicas y normativas

PARTE INTEGRAL DEL ANEXO TÉCNICO

imagen de alta calidad) sin compresión cuando así sean solicitados y/o exigidos en el protocolo de transferencias.

R3.8. Registro local de información de representación. Para cada objeto digital, debe incluir capacidades para mantener un registro completo sobre las representaciones disponibles, sus estados técnicos, sus relaciones internas y la ubicación de sus archivos asociados. Esto debe incluir derivaciones, versiones, copias maestras, copias de acceso y cualquier transformación autorizada.

R3.9. Asociación obligatoria de metadatos de preservación. Cada objeto digital aceptado debe contar con metadatos PREMIS[60] que incluyan:

- Eventos de preservación,
- Agentes involucrados,
- Derechos aplicables,
- Características técnicas,
- Resultados de validaciones y
- Cualquier acción realizada sobre el objeto digital.

Este registro constituye el núcleo de la historia de preservación del Paquete de Información de Archivo (PIA).

R3.10. Verificación de integridad durante la conversión del Paquete de Información de Transferencia (PIT) en Paquete de Información de Archivo (PIA). Debe incluir capacidades para recalcular y contrastar los valores de hash[61], identificando alteraciones, pérdidas, corrupción silenciosa o inconsistencias surgidas durante la admisión. Los resultados deben registrarse como eventos PREMIS.

R3.11. Mecanismos independientes de verificación de integridad. Además del control interno, el repositorio debe incluir capacidades que brinden mecanismos externos o redundantes (hash secundario, verificación cruzada, auditorías periódicas, controles de bit-level) para reforzar la confianza en los resultados de integridad y mitigar riesgos técnicos.

R3.12. Documentación y reporte sistemático de todas las acciones de preservación. Debe incluir capacidades que permitan que toda acción automatizada o manual asociada a preservación tales como:

- Migración,
- Normalización,
- Validación,
- Verificación,
- Corrección,
- Enriquecimiento de metadatos,
- Monitoreo de formatos

Quede registrada, documentada y disponible para auditoría, asegurando la transparencia del proceso y fortaleciendo la gobernanza del repositorio.

R3.12. El sistema deberá transformar los PI aceptados en Paquetes de Información de Archivo (PIA), garantizando la preservación de la autenticidad, integridad y trazabilidad.

[60] Ver glosario en 3.4.2 Directrices técnicas y normativas

[61] Ver glosario en 3.4.2 Directrices técnicas y normativas

PARTE INTEGRAL DEL ANEXO TÉCNICO

R3.13. Esta transformación deberá ser completamente automatizada y documentada, registrando en PREMIS los eventos, agentes y resultados asociados.

R3.14. El repositorio deberá permitir el control de versiones de los PIA, incluyendo esquemas, configuraciones y metadatos, con mecanismos claros de trazabilidad y protocolos de reversión ante errores o fallas. Asimismo, deberá preservar las propiedades significativas y transformacionales críticas de los objetos digitales, especialmente cuando se realicen procesos de normalización o migración inicial.

R4. Requisitos de Planificación de la Preservación

En el marco del proceso de Planificación de la Preservación definido por el modelo OAIS, el Archivo General de Bogotá debe contar con mecanismos formales que permitan anticipar riesgos, evaluar el estado de los objetos digitales y ejecutar acciones que aseguren su sostenibilidad en el tiempo. Este componente es esencial para garantizar que los objetos digitales preserven su valor probatorio, administrativo e histórico aun frente a cambios tecnológicos, variación de formatos, deterioro de medios o fallas de infraestructura.

Con base en ello, se establecen los siguientes requisitos:

R4.1. Estrategias de preservación definidas y actualizadas. Debe incluir capacidades para permitir la adopción y mantenimiento de estrategias de preservación claramente documentadas, alineadas con los estándares internacionales (NTC-ISO 14721[62], PREMIS[63], NTC-ISO 16363[64]) y con las directrices institucionales del Archivo General de Bogotá. Estas estrategias deben contemplar acciones como migración, normalización, monitoreo de formatos, controles de integridad, redundancias y mecanismos de recuperación ante fallos. Su actualización debe hacerse de manera periódica, considerando resultados del diagnóstico técnico, vigilancia tecnológica como un proceso continúo usando fuentes específicas (ej. NARA[65]) y análisis de riesgos del repositorio.

R4.2. Monitoreo y notificación de obsolescencia o corrupción. Debe contar con herramientas que permitan identificar alertas asociadas al deterioro, riesgo o pérdida de integridad de los objetos digitales, incluyendo:

- Incompatibilidad o inestabilidad de formatos;
- Fallas en el cálculo de hashes;
- Detección de corrupción silenciosa de datos (bit rot)[66];
- Obsolescencia de software;
- Códecs[67]
- Dependencias técnicas.

Deberá generar notificaciones automáticas y reportes accesibles para el equipo de preservación, permitiendo una reacción inmediata ante riesgos detectados con formatos

[62] Ver referentes internacionales y nacionales en 3.4.2 Directrices técnicas y normativas
[63] Ver glosario en 3.4.2 Directrices técnicas y normativas
[64] Ver referentes internacionales y nacionales en 3.4.2 Directrices técnicas y normativas
[65] Ver glosario en 3.4.2 Directrices técnicas y normativas
[66] Ver glosario en 3.4.2 Directrices técnicas y normativas
[67] Ver glosario en 3.4.2 Directrices técnicas y normativas

de alto riesgo de obsolescencia (ej. JPEG, MP3, VOB). formatos de preservación sin pérdida (ej. PDF/A[68], TIFF[69], WAV[70]).

R4.3. Ajuste dinámico de los planes de preservación. Como resultado del monitoreo, debe incluir capacidades para ofrecer la posibilidad de actualizar, corregir o redefinir los planes de preservación asociados a cada tipo de objeto digital, fondo o colección. Esto incluye la activación de procesos de migración, la modificación de reglas de almacenamiento, la actualización de metadatos de preservación, la redefinición de copias de seguridad o la ejecución de estrategias de normalización. Los ajustes deben quedar documentados como eventos PREMIS[71] y conservar trazabilidad para auditorías futuras.

R4.4. Reportes sobre la efectividad de las acciones de preservación. Debe incluir capacidades para generar informes periódicos que evidencien:

- el estado general de preservación del repositorio,
- el nivel de cumplimiento de los planes establecidos y
- los resultados de las acciones preventivas o correctivas.

R4.5.El sistema deberá incorporar capacidades para la planificación activa de la preservación, incluyendo una política formal de migración que contemple distintos tipos de acciones: renovación, replicación, reempaquetado y transformación. Esta política deberá definir disparadores claros (obsolescencia, riesgos tecnológicos, cambios normativos) y procedimientos de evaluación y aceptación.

R4.6.Se deberán mantener mecanismos para la actualización continua de la base de conocimiento de la comunidad designada, incluyendo la definición de perfiles, pruebas de comprensibilidad y métricas que permitan validar que los PIA siguen siendo interpretables a lo largo del tiempo.

R4.7.El repositorio deberá garantizar almacenamiento seguro, redundante y escalable, con capacidad para gestionar millones de registros diarios sin degradación del servicio. Se deberán implementar controles automáticos de integridad, verificación periódica de hash y mecanismos de detección temprana de corrupción o pérdida de información.

R4.8.El sistema deberá soportar la ejecución de pruebas periódicas de recuperación ante desastres, documentando resultados, tiempos de recuperación y evidencias de restauración exitosa. Estas pruebas deberán alinearse con los planes de continuidad del Archivo General de Bogotá y las directrices de la OTIC.

Estos reportes deben permitir evaluar la efectividad de las estrategias implementadas, identificar tendencias de riesgo y orientar la toma de decisiones institucionales sobre la sostenibilidad tecnológica y operativa del Repositorio Archivístico Digital Confiable del Archivo General de Bogotá.

R5. Requisitos de almacenamiento y preservación

En el marco de las funciones de Almacenamiento Seguro y Preservación Activa definidas por el modelo OAIS, el Repositorio Digital del Archivo General de Bogotá debe

[68] Ver glosario en 3.4.2 Directrices técnicas y normativas

[69] Ver glosario en 3.4.2 Directrices técnicas y normativas

[70] Ver glosario en 3.4.2 Directrices técnicas y normativas

[71] Ver referentes internacionales y nacionales en 3.4.2 Directrices técnicas y normativas

PARTE INTEGRAL DEL ANEXO TÉCNICO

implementar mecanismos que garanticen la preservación íntegra, verificable y trazable de los objetos digitales a lo largo del tiempo. Para ello, se establecen los siguientes requisitos orientados al control, administración y seguimiento del almacenamiento, así como a la documentación de todas las intervenciones de preservación realizadas sobre los objetos digitales.

R5.1. Registro formal de estrategias de preservación. Debe incluir capacidades para permitir la documentación detallada de las estrategias de preservación definidas para cada clase de objeto digital, identificando:

- El tipo de acción,
- Su propósito,
- Condiciones de ejecución,
- Periodicidad y
- Responsables.

Este registro debe mantenerse actualizado y vinculado a los eventos PREMIS asociados a cada documento, asegurando transparencia y trazabilidad institucional.

R5.2. Programación, control y ejecución de acciones de migración y reorganización del almacenamiento. Debe ofrecer capacidades para programar y ejecutar:

- Migraciones controladas de formatos,
- Reorganizaciones de almacenamiento,
- Replicación entre ubicaciones y
- Verificación de copias seguras.

Cada acción debe registrarse como un evento de preservación, indicando versiones, fechas, algoritmos utilizados y resultados obtenidos. Debe incluir capacidades para permitir auditoría de estos procesos y así garantizar consistencia y confiabilidad.

R5.3. Conservación tanto del documento original como del derivado migrado. Siempre que se ejecute una migración de formato o conversión autorizada, debe incluir capacidades para conservar la copia original y la copia resultante, asegurando que ambas queden claramente diferenciadas y documentadas. Esta medida garantiza la recuperación ante fallos, la comparación retroactiva y la preservación de la autenticidad histórica del objeto digital.

R5.4. Monitoreo sistemático de integridad mediante algoritmos de hash. El repositorio debe contar con mecanismos permanentes de verificación de integridad, capaces de calcular y comparar valores hash[72] (SHA-256[73], o superior) para detectar corrupción silenciosa, alteraciones no autorizadas o errores de almacenamiento. Estos controles deben ejecutarse periódicamente y quedan registrados como eventos de preservación.

R5.5. Registro detallado de todas las acciones de preservación. Toda acción realizada sobre un objeto digital, migración, normalización, verificación de integridad, reorganización de almacenamiento, enriquecimiento de metadatos, replicación, restauración o cualquier intervención técnica debe ser registrada en metadatos de preservación. El sistema debe almacenar estos registros en formatos abiertos, asegurando trazabilidad completa del ciclo de vida del documento.

PARTE INTEGRAL DEL ANEXO TÉCNICO

[72] Ver glosario en 3.4.2 Directrices técnicas y normativas

[73] Ver glosario en 3.4.2 Directrices técnicas y normativas

R5.6. Prohibición de alteración del contenido documental posterior a la migración. El repositorio debe garantizar que ninguna acción de preservación implique modificación del contenido intelectual del documento. Las migraciones solo podrán transformar estructuras técnicas, sintácticas o de codificación, sin alterar el significado, la forma o la información contenida en el archivo. Cualquier intento de modificación debe ser bloqueado automáticamente y reportado como incidente.

R5.7. El repositorio deberá garantizar almacenamiento seguro, redundante y escalable, con capacidad para gestionar millones de registros diarios sin degradación del servicio. Se deberán implementar controles automáticos de integridad, verificación periódica de hash y mecanismos de detección temprana de corrupción o pérdida de información.

R5.8. El sistema deberá soportar la ejecución de pruebas periódicas de recuperación ante desastres, documentando resultados, tiempos de recuperación y evidencias de restauración exitosa. Estas pruebas deberán alinearse con los planes de continuidad del Archivo General de Bogotá y las directrices de la OTIC.

R6. Gestión de la Información Descriptiva

En el marco del componente de Gestión de Datos del modelo OAIS, el Repositorio Archivístico Digital Confiable del Archivo General de Bogotá debe asegurar que los metadatos asociados a cada Paquete de Información de Archivo (PIA) se administren de manera consistente, verificable y plenamente interoperable. La calidad y completitud de los metadatos son condiciones esenciales para garantizar la trazabilidad, la preservación y el acceso a los documentos electrónicos de archivo, tal como evidenciaron los análisis técnicos realizados sobre fondos y colecciones digitales.

Con este propósito, se establecen los siguientes requisitos funcionales:

R6.1. Configuración y administración de metadatos para procesos de búsqueda y recuperación. Debe contar con capacidades para permitir configurar y gestionar estructuras de metadatos que faciliten la búsqueda, localización y consulta de los objetos digitales mediante criterios descriptivos, técnicos, administrativos y de preservación. Esto incluye la definición de campos obligatorios, la compatibilidad con esquemas de referencia (Dublin Core[74], ISAD(G) [75], PREMIS[76], METS[77]) y la capacidad para indexar contenidos de manera eficiente.

R6.2. Captura y asociación de metadatos mínimos durante la admisión. Durante el proceso de ingreso (PIT) → (PIA), debe incluir capacidades para garantizar la captura de un conjunto mínimo de metadatos esenciales para la preservación, para asegurar que se acorta la brecha encontrada en los metadatos (64% de campos vacíos en promedio) Estos metadatos deben incluir:

A nivel Básico:

- Identificación del productor,
- Fecha de transferencia,
- Valores de integridad (hash)[78],

[74] Ver glosario en 3.4.2 Directrices técnicas y normativas
[75] Ver glosario en 3.4.2 Directrices técnicas y normativas
[76] Ver glosario en 3.4.2 Directrices técnicas y normativas
[77] Ver glosario en 3.4.2 Directrices técnicas y normativas
[78] Ver glosario en 3.4.2 Directrices técnicas y normativas

- Formato,
- Tamaño,
- Características técnicas y
- Referencias archivísticas.

A nivel de los campos claves de PREMIS[79]

- Agentes,
- Eventos,
- Derechos de autor,
- Resultados de validación de los anteriores

A nivel de ISAD(G)

- Historia Institucional
- Nivel de descripción
- Condiciones de Acceso
- Condiciones de uso
- Fechas: Fechas extremas de creación de los documentos

Debe contar con capacidades para validar su completitud antes de aceptar el paquete.

R6.3. Aseguramiento de integridad referencial entre el Paquete de información de Archivo (PIA) y sus metadatos. El repositorio debe mantener una relación verificable entre cada AIP y los metadatos asociados. Ningún Paquete de información de Archivo (PIA) podrá existir sin su respectivo registro de metadatos, y todas las representaciones del documento deberán estar vinculadas de manera consistente. Esta integridad referencial es fundamental para asegurar trazabilidad, autenticidad y coherencia archivística.

R6.4. Restauración de integridad referencial en caso de ruptura o inconsistencias. Debe incluir capacidades para validar situaciones donde se detecten inconsistencias como vínculos rotos, metadatos ausentes, archivos no asociados o discrepancias entre el Paquete de información de Archivo (PIA) y su METS/PREMIS debe contar con mecanismos para restaurar la integridad referencial. Esto incluye herramientas de:

- Diagnóstico,
- Registros de auditoría,
- Reconstrucción de enlaces y
- Validaciones automáticas posteriores,

Para ello debe dejar constancia de las acciones correctivas mediante eventos PREMIS.

R6.5. El sistema deberá ofrecer herramientas robustas para la creación, carga y edición de esquemas de clasificación archivística, asegurando su correspondencia con los instrumentos archivísticos institucionales (CCD, TRD y TVD). Deberá permitir la organización jerárquica de fondos, secciones, series, subseries, expedientes y tipos documentales.

R6.6. Se deberán definir plantillas reutilizables de metadatos, soportando estándares como Dublin Core, EAD, METS y PREMIS, así como la asociación automática de archivos y carpetas a los paquetes correspondientes. El sistema deberá validar la coherencia semántica de los metadatos e incorporar documentación que facilite su interpretación independiente.

[79] Ver referentes internacionales y nacionales en 3.4.2 Directrices técnicas y normativas

PARTE INTEGRAL DEL ANEXO TÉCNICO

R7. Requisitos para la generación, control y distribución de Paquetes de información de Consulta (PIC)

La generación de Paquetes de información de Paquetes de Información de Consulta (PIC)[80] constituye una etapa esencial para garantizar el acceso controlado, seguro y verificable a objetos digitales preservados en el Repositorio Archivístico Digital Confiable del Archivo General de Bogotá. Esta fase debe asegurar que los objetos digitales difundidos mantengan su autenticidad, correspondan fielmente a los contenidos custodiados en los Paquetes de información de Archivo (PIA) y cumplan con las restricciones, autorizaciones y políticas de acceso definidas para cada fondo, serie o tipo documental. En coherencia con ello, se establecen los siguientes requisitos:

R7.1. Implementación y mantenimiento de una política de registro de accesos. Debe contar con una política formal de registro de accesos, ajustada a los niveles de seguridad y control requeridos tanto por el Archivo General de Bogotá como por los productores (entre los que se encuentran las entidades vigiladas) o depositantes de los documentos. Esta política debe definir qué información se registra, cómo se conserva, quién puede consultarla y por cuánto tiempo, garantizando trazabilidad y capacidad de auditoría.

R7.2. Acceso a los Paquetes de información de Archivo (PIA) exclusivamente por usuarios autorizados. Debe contar con capacidades para asegurar que únicamente los usuarios con permisos válidos puedan acceder a los paquetes PIA, conforme a los acuerdos documentados con las entidades productoras. Esto incluye la obligación de:

- Respetar restricciones legales,
- Derechos de autor,
- Cláusulas de reserva,
- Lineamientos de protección de datos personales y
- Condiciones especiales establecidas en los convenios de transferencia.

R7.3. Configuración e implementación de políticas de acceso basadas en identidad y autenticación. Debe contar con capacidades para permitir definir, documentar y operar políticas de acceso diferenciadas, que pueden ir desde la consulta libre sin identificación del usuario, hasta controles estrictos basados en autenticación multifactor, según los acuerdos entre el repositorio y los productores. Estas políticas deben quedar integradas al sistema y ser aplicadas de forma automática en cada solicitud de acceso.

R7.4. Registro y análisis de fallos de control de acceso. Debe contar con capacidades que permitan registrar todos los incidentes relacionados con accesos denegados de manera incorrecta, fallas de autenticación o cualquier evento que sugiera problemas en el control de seguridad. Dichos registros deben ser analizados periódicamente para identificar vulnerabilidades, inconsistencias o errores en la configuración del sistema.

R7.5. Validación y previsualización del contenido solicitado por el usuario. Debe contar con mecanismos que permitan verificar que el Paquete de Información de Consulta (PIC) generado corresponde de manera exacta a la solicitud del usuario. Esto incluye funciones de previsualización o revisión previa que permitan confirmar integridad, completitud y pertinencia, garantizando que el usuario reciba únicamente lo que ha solicitado.

[80] Ver glosario en 3.4.2 Directrices técnicas y normativas

COPIA CONTROLADA DEL ANEXO TÉCNICO

R7.6. Garantía de correspondencia entre el PIC generado y la solicitud del usuario. El proceso de construcción del Paquete de Información de Consulta (PIC) debe asegurar que el contenido entregado coincida con los parámetros solicitados:

- Tipo de documento,
- Rango temporal,
- Formato de salida,
- Calidad,
- Número de archivos.

Si el sistema ofrece diversas alternativas (por ejemplo, imágenes en JPG[81] o PNG[82]), el usuario debe recibir exactamente el formato requerido.

R7.7. Generación de reportes de aceptación o rechazo de solicitudes. Debe contar con capacidades para emitir notificaciones e informes sobre la aceptación, rechazo o requerimientos adicionales relacionados con las solicitudes de acceso. Los reportes deben explicar el motivo de la decisión, documentar la evidencia asociada y registrar el evento en los metadatos administrativos para garantizar trazabilidad.

R7.8. Garantía de autenticidad del Paquete de Información de Consulta (PIC) y trazabilidad con el Paquete de Información de Archivo (PIA). Debe contar con capacidades para asegurar que los PIC entregados sean copias auténticas del contenido original o que dispongan de una cadena de trazabilidad verificable entre el PIA y el PIC generado. Para ello, debe contar con capacidades para poder demostrar auditivamente el proceso de construcción del PIC, incluyendo valores de integridad, procedimientos aplicados, origen del contenido y metadatos asociados. Este requisito es fundamental para sostener el valor probatorio, histórico y archivístico de los documentos puestos a disposición del usuario.

R7.9. El repositorio deberá permitir la generación controlada de Paquetes de Información de Consulta (PIC), activados por eventos específicos como solicitudes de acceso, publicaciones, procesos de difusión o interoperabilidad con otros sistemas.

R7.10. Se deberán gestionar formalmente los Order Agreements, definiendo condiciones de acceso, restricciones, licencias y formatos de entrega. El sistema deberá garantizar que los PIC mantengan la integridad y autenticidad de la información, diferenciando claramente entre los objetos preservados y las copias de consulta.

R8. Seguridad y Administración de Paquetes

R8.1. Gestión del número de copias y control de su ubicación. Debe incluir capacidades para administrar de manera precisa la cantidad de copias existentes de cada objeto digital, así como la ubicación de cada una de ellas, ya sea local, remota o en sitios de contingencia. Este control debe registrarse en metadatos de preservación y permitir auditoría, asegurando que las copias cumplan con las políticas de redundancia definidas por el Archivo General de Bogotá.

R8.2. Sincronización consistente entre las copias del mismo documento. Debe garantizar que cualquier cambio intencional, validado y autorizado que se realice en una copia como la actualización de un metadato, la ejecución de una migración o la

[81] Ver glosario en 3.4.2 Directrices técnicas y normativas

[82] Ver glosario en 3.4.2 Directrices técnicas y normativas

PARTE INTEGRAL DEL ANEXO TÉCNICO

normalización de un archivo se replique en las demás copias almacenadas. Esta sincronización debe ser automática, verificable y registrada como evento PREMIS.

R8.3. Implementación de mecanismos para detectar corrupción o pérdida de bits. Debe contar con herramientas que permitan identificar deterioro, fragmentación o corrupción silenciosa de datos (bit rot)[83], mediante verificaciones de integridad periódicas y controles redundantes basados en algoritmos de hash[84]. Estas verificaciones deben aplicarse tanto a copias primarias como secundarias.

R8.4. Generación de reportes y acciones frente a incidentes de corrupción o pérdida de datos. Debe contar con capacidades para registrar y notificar cualquier anomalía detectada en la integridad de los objetos digitales, generando reportes de incidente que detallen la causa, alcance, archivos afectados y acciones de recuperación aplicadas. Deberá contar con capacidades para activar mecanismos de reparación o sustitución basados en copias confiables, manteniendo documentación de todo el proceso.

R8.5. Implementación de políticas de actualización y migración asociadas a la vida útil del hardware. Debe contar con políticas claras que regulen la actualización, renovación y migración de los componentes de hardware, considerando la vida útil del soporte físico y el riesgo de obsolescencia tecnológica. Estas políticas deben incluir planes periódicos de reemplazo, pruebas de compatibilidad, validaciones de integridad posteriores y análisis comparativo de desempeño.

R8.6. Gestión documentada de cambios críticos y pruebas de impacto. Debe incluir capacidades que le permitan documentar formalmente la gestión de cambios que impacten procesos críticos del repositorio, tales como:

- actualizaciones de software,
- modificación de arquitecturas de almacenamiento,
- ajustes en políticas de preservación o
- cambios en protocolos de seguridad.

Asimismo, deberán implementarse procedimientos para evaluar el efecto de dichos cambios, mediante pruebas controladas antes de su adopción definitiva.

R8.7. Evaluación de riesgos y beneficios en decisiones de actualización de software de seguridad. Toda actualización relacionada con componentes de seguridad incluidos sistemas operativos, módulos de autenticación, firewalls, servicios de cifrado o sistemas de detección de intrusiones debe evaluarse documentando sus riesgos, beneficios y posibles impactos en la estabilidad del repositorio. Esta evaluación deberá formar parte del expediente técnico del sistema y ser usada como insumo para decisiones estratégicas.

R8.8. El sistema deberá contar con una interfaz web de administración y acceso, moderna, responsiva y amigable, con soporte multilingüe y criterios de accesibilidad. Esta interfaz deberá incluir un panel de control con indicadores clave, monitoreo en tiempo real y métricas exportables sobre uso, integridad, transferencias y accesos.

PARTE INTEGRAL DEL ANEXO TÉCNICO

[83] Ver glosario en 3.4.2 Directrices técnicas y normativas

[84] Ver glosario en 3.4.2 Directrices técnicas y normativas

R8.9. Se deberá permitir la gestión de usuarios y grupos con roles diferenciados, auditoría específica para los procesos de ingesta y difusión, y control de versiones de paquetes, esquemas y configuraciones. Asimismo, el sistema deberá ofrecer capacidades avanzadas de interoperabilidad (OAI-PMH, APIs, autenticación federada), gestión de licencias y políticas de almacenamiento, asegurando siempre la trazabilidad y el cumplimiento normativo.

4.4 Requisitos No Funcionales

R9. Seguridad

La seguridad de la información y la confiabilidad operativa constituyen pilares esenciales para garantizar la preservación a largo plazo de los documentos electrónicos de archivo custodiados por el Archivo General de Bogotá. El repositorio debe operar bajo parámetros estrictos de protección, control de accesos, cifrado, auditoría y continuidad, de acuerdo con las políticas institucionales, los estándares internacionales y las exigencias del entorno tecnológico distrital.

Con este propósito, se establecen los siguientes requisitos:

R9.1. Cifrado de todas las comunicaciones. El repositorio debe garantizar que toda transmisión de información tanto interna como externa se realice mediante protocolos de cifrado robustos, tales como IP-SEC[85], 3DES[86], AES[87] o SSL/TLS[88], con llaves criptográficas de mínimo 128 bits. Este requisito busca proteger la información archivística de interceptaciones, accesos no autorizados y ataques de intermediario.

R9.2. Implementación de mecanismos de interoperabilidad estándar. El sistema debe permitir la interoperación con otros servicios institucionales y distritales a través de protocolos abiertos como XML[89], SOAP[90] o REST[91], facilitando integraciones seguras con SGDEA, plataformas de autenticación, sistemas de transferencia digital y servicios de consulta.

R9.3. Copias de seguridad y restauración automatizadas. Debe contar con procedimientos automáticos de backup y restauración, coherentes con el Plan de Recuperación de Sistemas y con las políticas institucionales de continuidad operativa de la Oficina de las Tecnologías de la Información y las Comunicaciones OTIC. Estos procesos deben ejecutarse sin intervención manual y estar documentados.

R9.4. Programación de rutinas y frecuencia de copias de seguridad. Debe permitir programar la periodicidad y alcance de las copias de seguridad, definiendo horarios, elementos a respaldar, retención de copias y validación de integridad posterior.

R9.5. Selección granular de elementos para respaldo. Debe ser posible elegir, de manera específica, los elementos, entidades, colecciones o espacios del repositorio que serán sometidos a copia de seguridad, permitiendo planes diferenciados según criticidad y volumen.

[85] Ver glosario en 3.4.2 Directrices técnicas y normativas
[86] Ver glosario en 3.4.2 Directrices técnicas y normativas
[87] Ver glosario en 3.4.2 Directrices técnicas y normativas
[88] Ver glosario en 3.4.2 Directrices técnicas y normativas
[89] Ver glosario en 3.4.2 Directrices técnicas y normativas
[90] Ver glosario en 3.4.2 Directrices técnicas y normativas
[91] Ver glosario en 3.4.2 Directrices técnicas y normativas

PARTE INTEGRAL DEL ANEXO TÉCNICO

R9.6. Restricción de conexiones por dirección IP. Debe contar con capacidades para permitir restringir el acceso mediante listas seguras de direcciones IP autorizadas. Asimismo, toda transmisión deberá utilizar el protocolo TCP/IP asegurando transporte confiable y protección de datos entre los distintos componentes distribuidos en la red.

R9.7. Restauración exclusiva por usuarios administradores. La restauración de datos solo podrá ser realizada por usuarios con perfil de administrador. En caso de error durante el proceso, debe contar con capacidades para detener la restauración y notificar inmediatamente al responsable para evitar daños mayores.

R9.8. Seguridad y control de acceso en bases de datos. Debe contar con capacidades para implementar mecanismos de control de acceso basados en roles, perfiles y privilegios claramente definidos. Ningún usuario no autorizado podrá tener permisos administrativos. El acceso a tablas, vistas, índices u otros objetos deberá estar estrictamente regulado.

R9.9. Manejo seguro de contraseñas. Las contraseñas no podrán almacenarse en texto plano. Deben mantenerse cifradas mediante algoritmos unidireccionales reconocidos, como MD5, SHA-128 o SHA-256[92], con llaves mínimas de 128 bits. La plataforma debe reforzar controles para prevenir vulneraciones.

R9.10. Protección contra ataques mediante inyección o ejecución de código. Debe contar con capacidades para garantizar la validación segura de los datos recibidos desde formularios u otros puntos de entrada para evitar que un atacante ejecute código malicioso o comprometa el sistema.

R10. Auditoría y Trazabilidad

R9.11. Pistas de auditoría inalterables. Debe conservar pistas de auditoría que no puedan ser modificadas o eliminadas, registrando toda acción relacionada con los objetos digitales o con cualquier nivel, incluso para la Tabla de Retención Documental y Cuadro de Clasificación Documental.

R9.12. Captura automática de eventos de auditoría. Todos los registros deben generarse automáticamente, sin intervención del usuario, incluyendo:

- Fecha,
- Hora,
- Usuario,
- Tipo de acción,
- Resultado e identificación del recurso afectado.

R9.13. Conservación de auditorías según los tiempos de retención. Las pistas de auditoría deben mantenerse de acuerdo con los tiempos establecidos en las TRD/TVD[93] aplicables, garantizando que su conservación acompañe los procesos documentales asociados.

R11. Disponibilidad, Eficiencia Operativa e Interoperabilidad

[92] Ver glosario en 3.4.2 Directrices técnicas y normativas

[93] Ver glosario en 3.4.2 Directrices técnicas y normativas

PARTE INTEGRAL DEL ANEXO TÉCNICO

R9.14. Disponibilidad del servicio conforme a acuerdo de nivel (SLA[94]) del 99,6 %. Debe garantizar disponibilidad permanente, asegurando continuidad operativa y capacidad de respuesta oportuna para consultas, transferencias y procesos de preservación.

R9.15. Tiempo máximo de inactividad no programada. No debe superar doce (12) horas de inactividad mensual no prevista. Los mantenimientos programados deben realizarse en horarios no hábiles, evitando impactos en consultas o procesos institucionales.

R9.16. Seguridad en servicios web e interfaces de interoperabilidad. Toda interacción a través de servicios web, APIs[95] u otros mecanismos de interoperación debe cumplir con estándares de seguridad para evitar accesos indebidos o filtración de datos sensibles.

R9.17. Herramienta de auditoría para control de actualizaciones. Debe contar con una herramienta que registre todas las acciones realizadas por usuarios sobre el sistema:

- Fecha,
- Hora,
- Identificación del usuario y
- Tipo de actualización.

R9.18. Control de sesiones y tiempos de inactividad. Debe implementar mecanismos que cierren automáticamente sesiones inactivas en un tiempo definido por política que no debería superar los 5 minutos, evitando accesos indebidos o uso fraudulento por abandono de sesión.

R9.19. Acceso multiplataforma y compatibilidad con navegadores. Debe ser accesible desde Windows, Linux, macOS y desde los navegadores más utilizados: Firefox, Chrome, Safari, Opera y aquellos compatibles en dispositivos móviles y tabletas.

R9.20. Cumplimiento de estándares W3C y lineamientos de accesibilidad. La solución debe estar alineada con las directrices W3C[96] y las políticas de Gobierno Digital, garantizando accesibilidad para personas con discapacidad y la correcta visualización en diversos dispositivos y tecnologías asistidas.

R9.21. Disponibilidad de ayudas en línea y documentación en español. Debe ofrecer manuales de usuario, guías de administración y ayudas contextuales en idioma español, integradas directamente en la plataforma.

R9.22. Diseño responsive. Debe contar con una interfaz adaptable a distintos tamaños de pantalla, garantizando una experiencia adecuada en equipos de escritorio, tabletas y dispositivos móviles.

PARTE INTEGRAL DEL ANEXO TÉCNICO

R12. Interfaz, Configuración y Administración

Para garantizar el correcto funcionamiento del Repositorio Archivístico Digital Confiable y asegurar que la plataforma responda a las necesidades de preservación, consulta, operación, interoperabilidad y sostenibilidad tecnológica del Archivo General de Bogotá, se establecen los siguientes requisitos adicionales. Estos lineamientos complementan las capacidades exigidas para un ecosistema tecnológico robusto, seguro y adaptable,

[94] Ver glosario en 3.4.2 Directrices técnicas y normativas
[95] Ver glosario en 3.4.2 Directrices técnicas y normativas
[96] Ver glosario en 3.4.2 Directrices técnicas y normativas

capaz de operar bajo los estándares de preservación digital, gobierno digital y accesibilidad tecnológica.

R9.23. Interfaz gráfica para instalación y configuración. Debe ofrecer una interfaz gráfica integral que permita instalar, configurar y administrar todos los componentes de hardware y software, evitando dependencias de comandos complejos o configuraciones manuales que puedan generar riesgos operativos o de seguridad.

R9.24. Solución 100% web y administrable desde navegador. Toda la administración, parametrización y operación debe realizarse desde una plataforma web completamente funcional, accesible mediante navegador y sin requerir instalaciones locales. Esto facilita la centralización, reduce costos de mantenimiento y fortalece la seguridad.

R9.25. Accesibilidad multiplataforma y diseño adaptable. Debe ser accesible desde cualquier dispositivo móvil o de escritorio, con un diseño adaptable (“responsive”) que garantice la correcta visualización, navegación y operación desde teléfonos, tabletas y equipos portátiles.

R13. Reportes, Estándares y Almacenamiento

R9.26. Modelado de reportes según perfil y necesidad. Debe permitir la generación de reportes configurables, adaptados al perfil del usuario y a los niveles de acceso autorizados, garantizando que cada persona pueda visualizar únicamente la información pertinente a sus funciones.

R9.27. Compatibilidad con el estándar CMIS. La plataforma debe soportar de manera nativa el estándar CMIS[97] (Content Management Interoperability Services), permitiendo la interoperabilidad con gestores documentales, sistemas de archivo y plataformas externas que utilicen este protocolo.

R9.28. Manejo nativo de objetos BLOB. El sistema debe soportar el almacenamiento, administración y recuperación de objetos BLOB (Binary Large Objects) sin pérdidas de rendimiento, garantizando la preservación de archivos de gran tamaño o formatos complejos.

R9.29. Compatibilidad con diferentes arquitecturas de almacenamiento. El repositorio debe operar de forma nativa sobre infraestructuras NAS (Network Area Storage), SAN (Storage Area Network) y DAS (Direct Attached Storage), permitiendo flexibilidad en la administración y escalabilidad según las capacidades tecnológicas del Archivo General de Bogotá.

R14. Integración, Sincronización y Operación en Tiempo Real

R9.30. Integración completa entre módulos y componentes. Todos los subsistemas que lo conforman deben operar de manera completamente integrada, permitiendo el intercambio de información en línea y la sincronización adecuada entre procesos de ingesta, preservación, acceso y auditoría.

R9.31. Soporte para ambientes virtualizados. La plataforma debe ser compatible con arquitecturas virtualizadas, permitiendo su despliegue en entornos de virtualización o equivalentes, garantizando flexibilidad operativa y optimización del uso de recursos.

[97] Ver glosario en 3.4.2 Directrices técnicas y normativas

PARTE INTEGRAL DEL ANEXO TÉCNICO

R9.32. Interfaz gráfica orientada al usuario final. Deben incluir capacidades para ofrecer una experiencia clara y fácil de usar, con flujos de navegación coherentes con los procesos archivísticos y de preservación definidos por el Archivo General de Bogotá.

R15. Escalabilidad, Arquitectura y Compatibilidad

R9.33. Escalabilidad y arquitectura de 64 bits. La solución debe ser escalable y estar basada en una arquitectura de 64 bits, habilitada para entornos de alta disponibilidad, clustering, replicación y mecanismos de balanceo de carga.

R9.34. Arquitectura basada en tres capas. El sistema debe implementar una arquitectura de mínimo tres capas independientes:

- Presentación,
- Lógica de negocio,
- Base de datos.

Esta separación asegura modularidad, seguridad y facilidad de mantenimiento.

R9.35. Independencia de la topología de red. La plataforma debe ser independiente de la red donde opere, funcionando adecuadamente en entornos LAN[98] y WAN[99], tanto en conexiones institucionales internas como en escenarios distribuidos.

R9.36. Conectividad con diferentes motores de bases de datos. Debe ser compatible, como mínimo, con Oracle, SQL Server, MySQL y PostgreSQL, permitiendo flexibilidad tecnológica y adaptación a la infraestructura existente.

R9.37. Disponibilidad de diccionario de datos técnico. Debe proveer un diccionario de datos detallado, describiendo cada tabla, campo, tipo de dato y valores configurados. Esta herramienta será esencial para administradores técnicos, auditorías y procesos de interoperabilidad.

R16. Interoperabilidad Avanzada y Comunicación Institucional

R9.38. Integración mediante servicios web. Debe ofrecer servicios web[100] robustos y seguros que permitan interoperar con otras plataformas institucionales o externas, bases de datos, SGDEA[101] o sistemas especializados.

R9.39. Integración con correo institucional. Debe integrarse con el correo electrónico institucional para permitir, de forma manual o automatizada, la recepción y envío de documentos, notificaciones u operaciones derivadas de la gestión archivística.

R9.40. Autenticación y administración de usuarios mediante directorio activo. Debe integrarse con servicios de directorio activo (LDAP[102]), permitiendo autenticación centralizada, administración de usuarios desde un repositorio institucional y sincronización directa con las políticas de seguridad organizacionales.

[98] Ver glosario en 3.4.2 Directrices técnicas y normativas
[99] Ver glosario en 3.4.2 Directrices técnicas y normativas
[100] Ver glosario en 3.4.2 Directrices técnicas y normativas
[101] Ver glosario en 3.4.2 Directrices técnicas y normativas
[102] Ver glosario en 3.4.2 Directrices técnicas y normativas

PARTE INTEGRAL DE ANEXO TÉCNICO

R17. Rendimiento

Para garantizar la operación eficiente del Repositorio Archivístico Digital Confiable y asegurar que responda a la demanda transaccional, de acceso y de uso concurrente propia del Archivo General de Bogotá, se establecen los siguientes requisitos orientados al desempeño, estabilidad y tiempo de respuesta del sistema:

R9.41. Procesamiento de transacciones por segundo (TPS). Debe ser capaz de procesar un número definido de transacciones por segundo, conforme al análisis técnico de carga, conectividad y concurrencia realizado por la Oficina de Tecnologías de la Información y las Comunicaciones OTIC[103]. Este rendimiento será evaluado mediante herramientas de Software Testeo, aplicadas específicamente a los servicios definidos, garantizando que los tiempos de respuesta cumplan con los parámetros establecidos.

R9.42. Operación con usuarios concurrentes. El sistema debe mantener un funcionamiento estable y sin degradación significativa del rendimiento cuando existan, como mínimo, 1000 usuarios con sesiones activas de manera simultánea, considerando operaciones como consultas, descargas, búsquedas, generación de reportes y procesos de preservación. Este requisito asegura que la plataforma pueda responder a escenarios reales de uso institucional, especialmente en procesos de transferencia, auditoría y consulta masiva.

R9.43. Actualización de datos en tiempo real. Los cambios realizados en la base de datos nuevos registros, actualizaciones de metadatos, modificaciones de permisos o resultados de procesos de preservación deben reflejarse automáticamente para todos los usuarios con autorización. El acceso a la información actualizada no debe superar dos segundos, garantizando consistencia, integridad y eficiencia en la interacción con los objetos digitales y sus metadatos asociados.

R18. Síntesis ampliada de los requisitos complementarios

Los requisitos R9.41–R9.43 fortalecen las capacidades del repositorio en materia de rendimiento, estabilidad y tiempo de respuesta, y se integran de manera coherente con los requisitos previos relacionados con la seguridad, arquitectura y accesibilidad de la plataforma:

Seguridad

- Cifrado completo de las comunicaciones mediante protocolos robustos.
- Control de accesos basado en roles, autenticación y directorios activos.
- Almacenamiento seguro de contraseñas bajo algoritmos unidireccionales.
- Registro inalterable de pistas de auditoría.
- Protección contra ataques, inyección de código y accesos indebidos.

Acceso

- Disponibilidad mínima del 99,6 % bajo un Acuerdo de Nivel de Servicios formalmente establecido.
- Compatibilidad con navegadores modernos y dispositivos móviles.

[103] Ver glosario en 3.4.2 Directrices técnicas y normativas

PARTE INTEGRAL DEL ANEXO TÉCNICO

- Accesibilidad alineada con los lineamientos W3C[104] y la política de Gobierno Digital.
- Diseño adaptable (responsive) para garantizar usabilidad multidispositivo.

Arquitectura tecnológica

- Solución completamente web, administrable desde navegador.
- Arquitectura escalable de 64 bits, con soporte para clustering y replicación.
- Infraestructura en tres capas independientes: presentación, lógica de negocio y base de datos.
- Compatibilidad con múltiples motores de base de datos: Oracle, SQL Server, MySQL y PostgreSQL.
- Integración mediante servicios web SOAP/REST y soporte CMIS.
- Operación sobre entornos virtualizados y almacenamiento NAS[105], SAN[106] y DAS[107].

Rendimiento

- Procesamiento eficiente de transacciones mediante pruebas de carga certificadas.
- Operación con usuarios concurrentes sin degradación perceptible.
- Tiempos de respuesta inferiores a dos segundos en operaciones críticas.
- Escalabilidad para responder a incrementos progresivos de demanda institucional.

4.5 Plan de acción y ruta de implementación

El Modelo de Requisitos Tecnológicos definido para el proyecto de preservación digital del Archivo General de Bogotá se sustenta en una ruta de implementación progresiva, concebida para asegurar que la transición hacia un repositorio digital confiable se realice de manera ordenada, verificable y ajustada a las capacidades reales de la entidad. Este enfoque gradual está orientado a consolidar, en cada etapa, los elementos técnicos, archivísticos y operativos indispensables para garantizar la preservación a largo plazo de los documentos electrónicos de archivo del Distrito Capital.

La primera fase de esta ruta contempla la consolidación de los fundamentos técnicos, archivísticos y administrativos. En este momento inicial se formalizan las políticas internas de preservación digital, se actualizan los lineamientos institucionales y se establecen los procedimientos que regirán la admisión, el almacenamiento, el control de integridad, el monitoreo de formatos y el acceso a los documentos electrónicos. Asimismo, se definen los marcos de metadatos que serán utilizados para la preservación, incluyendo la adopción de esquemas como METS[108], PREMIS[109] y Dublin

[104] Ver glosario en 3.4.2 Directrices técnicas y normativas
[105] Ver glosario en 3.4.2 Directrices técnicas y normativas
[106] Ver glosario en 3.4.2 Directrices técnicas y normativas
[107] Ver glosario en 3.4.2 Directrices técnicas y normativas
[108] Ver glosario en 3.4.2 Directrices técnicas y normativas
[109] Ver glosario en 3.4.2 Directrices técnicas y normativas

PARTE INTEGRAL DEL ANEXO TÉCNICO

Core[110], así como las reglas para la identificación, empaquetamiento y conformación de los paquetes PIT[111], PIA[112] y PIC[113]. Esta etapa también exige la conformación de mecanismos de gobernanza y comités institucionales responsables del seguimiento, evaluación y mejora continua del repositorio, asegurando así una base normativa y técnica estable para el desarrollo del proyecto.

Superado este punto, la implementación avanza hacia la adecuación e instalación de la infraestructura tecnológica necesaria para la operación del repositorio digital. Durante esta fase se despliegan, configuran y prueban los componentes de software y hardware definidos en el proyecto, entre ellos los sistemas de almacenamiento, servidores, herramientas de validación y módulos de preservación. También se garantiza la integración con los sistemas institucionales existentes como plataformas de radicación, sistemas de gestión documental y servicios de firma digital, lo que permite el establecimiento de flujos de interoperabilidad seguros, trazables y auditables entre las entidades productoras y el Archivo General de Bogotá. Paralelamente, se ejecutan pruebas rigurosas de rendimiento, estabilidad, integridad, seguridad y recuperación ante fallos, necesarias para certificar la confiabilidad del sistema antes de su puesta en marcha en ambiente productivo.

Una vez establecida la infraestructura, la ruta de implementación contempla el alistamiento, tratamiento y preparación de los documentos electrónicos que serán incorporados al repositorio. En esta fase se desarrollan actividades de depuración y normalización de archivos digitales, atendiendo a los formatos, estructuras y metadatos identificados en el diagnóstico técnico. Igualmente, se verifican controles de integridad, se identifican riesgos tecnológicos, se eliminan duplicidades y se construyen los paquetes de información conforme a los lineamientos del modelo OAIS. La priorización de fondos, series y colecciones se realiza con base en criterios archivísticos y técnicos, tales como el valor documental, el nivel de riesgo, la obsolescencia tecnológica y las necesidades de acceso y consulta institucional. Este proceso garantiza que únicamente documentos preparados bajo estándares uniformes ingresen al repositorio.

De forma paralela, el proyecto integra un componente fundamental: el fortalecimiento institucional y el desarrollo de capacidades para los equipos técnicos responsables de la gestión documental y tecnológica. Esta fase abarca procesos de formación especializada en preservación digital, modelos OAIS y NDSA, empaquetamiento METS/PREMIS[114], flujos PIT/PIA/PIC[115] y protocolos de continuidad operativa. Además, incluye la elaboración de manuales, guías y lineamientos operativos para estandarizar procedimientos y asegurar que la operación del repositorio no dependa únicamente de la tecnología, sino también del conocimiento y la competencia del talento humano que lo administra.

Finalmente, la ruta culmina con el despliegue progresivo del repositorio digital en ambiente productivo, acompañado de un esquema de monitoreo continuo y mejora permanente. En esta fase se realiza un seguimiento constante a los indicadores de rendimiento, disponibilidad, interoperabilidad e integridad, así como a los patrones de uso por parte de las entidades y de los usuarios internos. Se desarrollan auditorías periódicas, evaluaciones técnicas y revisiones integrales que permiten corregir desviaciones, robustecer los procedimientos y garantizar la sostenibilidad del sistema.

[110] Ver glosario en 3.4.2 Directrices técnicas y normativas
[111] Ver glosario en 3.4.2 Directrices técnicas y normativas
[112] Ver glosario en 3.4.2 Directrices técnicas y normativas
[113] Ver glosario en 3.4.2 Directrices técnicas y normativas
[114] Ver glosario en 3.4.2 Directrices técnicas y normativas
[115] Ver glosario en 3.4.2 Directrices técnicas y normativas

Asimismo, el modelo de requisitos tecnológicos se actualiza con base en cambios normativos, avances tecnológicos y nuevas necesidades institucionales, asegurando que la solución evolucione conforme a los retos y expectativas del Distrito Capital.

En conjunto, esta ruta de implementación asegura que el Archivo General de Bogotá cuente con un repositorio digital sólido, auditable, escalable y plenamente alineado con los requerimientos contemporáneos de la preservación digital, consolidando así las bases para proteger la memoria institucional y garantizar el acceso al patrimonio documental electrónico a largo plazo.

V. RECURSOS Y SOSTENIBILIDAD

5.1 Presupuesto estratégico

La puesta en marcha del sistema de preservación digital del Archivo General de Bogotá exige una planificación financiera sólida y coherente con los objetivos técnicos e institucionales del proyecto. Para ello, se definió un presupuesto estratégico que contempla tres horizontes de acción: formulación, implementación y sostenibilidad alineados con el Marco de Gasto de Mediano Plazo (MGMP) del Distrito y con los instrumentos internos de planeación del Archivo General de Bogotá.

Los detalles se encuentran en el documento 3.4.6 Proyección de costos tecnológicos que justifica lo requerido para la gestión de la Arquitectura tecnológica tal como lo establece la norma técnica NTC-ISO 16363.

Este enfoque permitió identificar de manera clara los recursos necesarios en materia tecnológica, humana y operativa, garantizando que la construcción y puesta en marcha del repositorio digital cuenten con la financiación requerida y que su operación futura pueda mantenerse sin interrupciones.

Componente	Descripción general	Horizonte temporal	Responsable principal
Formulación	Comprende el diseño metodológico, la elaboración de instrumentos técnicos, la definición de lineamientos normativos, la consolidación del modelo de madurez y el análisis de requisitos.	Corto plazo 2026–2027)	Subdirección de Fortalecimiento Institucional – ARCHIVO GENERAL DE BOGOTÁ
Implementación	Incluye el desarrollo de la arquitectura conceptual y tecnológica, la adecuación e integración de infraestructura, y la puesta en marcha de estrategias de migración, metadatos y preservación digital.	Mediano plazo (2026–2027)	Oficina de Tecnologías de la Información (OTIC) – Secretaría General
Sostenibilidad	Comprende las actividades permanentes de mantenimiento,	Largo plazo	Subdirección de gestión del Patrimonio

PARTE INTEGRAL DEL ANEXO TÉCNICO

Componente	Descripción general	Horizonte temporal	Responsable principal
	actualización tecnológica, monitoreo, formación de equipos, auditoría y fortalecimiento de capacidades en preservación digital.	(2026–2030)	Documental / Archivo General de Bogotá / Grupo de Preservación Digital

5.2 Sostenibilidad institucional y tecnológica

La sostenibilidad del sistema de preservación digital del Archivo General de Bogotá se concibe como un proceso continuo que requiere la participación coordinada de las áreas técnicas, archivísticas y administrativas de la entidad. Para ello se estructuró un enfoque basado en tres ejes estratégicos que permiten garantizar la permanencia, escalabilidad y actualización del modelo de preservación a largo plazo:

1. Fortalecimiento del capital humano

El Archivo General de Bogotá ha promovido la formación especializada en preservación digital, gestión de riesgos, metadatos y estándares internacionales, fortaleciendo las capacidades internas mediante espacios de capacitación como el diplomado *Patrimonio Documental Digital* y otros procesos de actualización ofrecidos a los equipos técnicos y archivísticos. Esta inversión en talento humano garantiza que el conocimiento requerido para administrar y evolucionar el repositorio digital se mantenga dentro de la institución y se renueve periódicamente.

2. Actualización tecnológica planificada

La sostenibilidad tecnológica requiere de políticas de renovación periódica de hardware, software y herramientas de preservación, evitando la obsolescencia y garantizando la compatibilidad con estándares abiertos. El modelo contempla la adopción de buenas prácticas en gestión de infraestructura, verificación de integridad, control de versiones, seguridad digital y monitoreo de formatos, asegurando que las plataformas tecnológicas evolucionen de manera consistente con los cambios del entorno digital.

3. Planeación institucional y financiera

La preservación digital fue incorporada como un componente permanente de la planeación institucional del Archivo General de Bogotá, lo que permite asegurar la asignación anual de recursos técnicos, operativos y humanos necesarios para su operación. Este enfoque facilita la continuidad del sistema en el mediano y largo plazo, articulándolo con los procesos de inversión pública y con los lineamientos estratégicos del Distrito.

COPIA INTEGRAL DEL ANEXO TÉCNICO

VI. SEGUIMIENTO, EVALUACIÓN E IMPACTO

El modelo define un marco de seguimiento y evaluación sustentado en indicadores estratégicos que permiten medir el avance institucional, la efectividad técnica y la sostenibilidad del sistema de preservación digital. Estos mecanismos fortalecen la toma de decisiones, permiten ajustar procedimientos y garantizan que la implementación del modelo avance de manera ordenada y verificable.

6.1 Mecanismos de evaluación y revisión

Para asegurar una supervisión clara y coherente, se estableció una distribución de roles y responsabilidades agrupada en cinco categorías, conforme a la estructura institucional del Archivo General de Bogotá:

Grupo	Responsable
Preservación / Conservación	Subdirección de Patrimonio Documental
Tecnologías de la Información	Oficina de las Tecnologías de la Información y las Comunicaciones OTIC de la Alcaldía de Bogotá
Seguridad de la Información	Área especializada de la Oficina de las Tecnologías de la Información y las Comunicaciones OTIC
Subdirección del Sistema Distrital de Archivos	Dependencia del Archivo General de Bogotá
Comité Directivo	Dirección del Archivo General

Para cada actividad se definieron roles tipo RACI, permitiendo establecer quién ejecuta, quién aprueba, quién es consultado y quién debe mantenerse informado durante los procesos.

Leyenda de roles:

- **R – Responsable:** ejecuta la tarea.
- **A – Aprueba:** cuenta con la decisión final.
- **C – Consultado:** aporta criterios durante la ejecución.
- **I – Informado:** recibe actualizaciones y resultados.

Con base en estos roles, se estructuró la siguiente matriz RACI:

Proceso / Actividad	Preservación	TI	Seguridad	Subdirección del Sistema Distrital de Archivos	Comité Directivo
Definición de políticas y plan de preservación digital	R/A	C	C	C	A/I
Implementación del modelo OAIS y lineamientos AGN 01/24	R	R	C	C	I
Administración de metadatos y estándares (METS,	R/A	R	C	C	I

Proceso / Actividad	Preservación	TI	Seguridad	Subdirección del Sistema Distrital de Archivos	Comité Directivo
PREMIS, DC, ISO 23081)					
Gestión de la infraestructura tecnológica	C	R	C	–	I
Controles de seguridad digital y protección de datos	C	R	R/C	C	I
Validación legal de lineamientos	C	C	C	C	I
Auditorías internas y seguimiento	R	C	R	C	A/I
Aprobación de informes y planes	R	C	C	C	A/I
Definición de responsabilidades institucionales	R/A	C	C	C	A/I

6.2 Impacto esperado

La implementación del modelo de preservación digital generará impactos directos en la gestión documental y tecnológica del Archivo General de Bogotá, entre los cuales se destacan:

- Fortalecimiento de las capacidades institucionales para la preservación digital, integrando procesos, herramientas y talento humano especializado.
- Reducción significativa de riesgos tecnológicos, especialmente aquellos asociados a pérdida de información, fallas de integridad o obsolescencia.
- Aumento de la accesibilidad y disponibilidad de los fondos digitales para usuarios internos, entidades del Distrito y ciudadanía.
- Cumplimiento del marco normativo distrital y nacional, incluyendo estándares internacionales de preservación digital.
- Consolidación del Archivo General de Bogotá como referente técnico, articulando los componentes archivísticos, tecnológicos y de gobernanza para la protección del patrimonio digital de la ciudad.

Los indicadores definidos para esta evaluación son:

Categoría	Indicador	Método de medición	Periodicidad	Responsable
Cumplimiento	Ejecución del plan de preservación digital	(Actividades ejecutadas / planificadas) × 100	Semestral	Fortalecimiento Institucional – AGB[116]
Calidad	Completitud y consistencia de metadatos	% de objetos con metadatos completos	Anual	Subdirección de Patrimonio Documental del Distrito

[116] Ver glosario en 3.4.2 Directrices técnicas y normativas

PARTE INTEGRAL DEL ANEXO TÉCNICO

Categoría	Indicador	Método de medición	Periodicidad	Responsable
Impacto	Disponibilidad de fondos digitales	(Fondos accesibles / total fondos digitales) × 100	Anual	Subdirección de Patrimonio Documental del Distrito
Sostenibilidad	Actualización de infraestructura	(Componentes actualizados / planificados) × 100	Anual	OTIC[117] – Secretaría General
Riesgos	Reducción de riesgos críticos	(Riesgos mitigados / riesgos identificados) × 100	Anual	Seguridad de la Información – AGB

PARTE INTEGRAL DEL ANEXO TÉCNICO

[117] Ver glosario en 3.4.2 Directrices técnicas y normativas

VII. NOTAS ACLARATORIAS

El proceso de construcción del Modelo de Requisitos Tecnológicos consideró:

- Los insumos recopilados en los diagnósticos de fondos digitales, medios de almacenamiento y entidades distritales, consolidados en el entregable **3.4.1 Diagnóstico Integrado**.
- La adopción de un enfoque metodológico que garantiza rigor técnico, coherencia y progresividad.
- La articulación del documento como marco estratégico, normativo y operativo para el desarrollo de los entregables 3.4.3, 3.4.4, 3.4.5 y 3.4.6.
- La posibilidad de incorporar información complementaria durante la fase de cierre del proyecto, considerando los aportes derivados de la definición completa de la arquitectura tecnológica.

PARTE INTEGRAL DEL ANEXO TÉCNICO

VII. ANEXO

Matriz de Trazabilidad Requisito-Brecha-Norma (R-B-N).

Anexo estratégico del entregable 3.4.5. Modelo de Requisitos Tecnológicos, que tiene como objetivo demostrar cómo los requisitos funcionales y no funcionales (R) resuelven las brechas identificadas en el diagnóstico (B), cumpliendo con el marco normativo y los estándares de preservación (N).

Requisito (R)	Brecha Crítica del Diagnóstico (B)	Norma / Estándar de Referencia (N)	Impacto de No Cumplimiento / Riesgo Mitigado
R1. Estructura del Paquete de Información de transferencia (PIT) (Ej. Uso de UUID y formato METS.xml)	Inconsistencia Estructural y Nomenclatura: Uso de espacios en blanco, caracteres no normalizados, jerarquías no documentadas o inconsistentes en la mayoría de los fondos analizados.	Directriz de Normalización (3.4.2); OAIS (NTC-ISO 14721) (Estructura del Paquete de Información); METS (Estructura de empaquetamiento).	Falla de interoperabilidad con sistemas automatizados; pérdida de la unidad intelectual y dificultad en la automatización de flujos archivísticos.
R2. Requisitos para la Admisión (Ej. Validación de completitud de metadatos mínimos y rechazo de PITs no conformes)	Brecha Crítica de Metadatos: Diligenciamiento parcial (22% - 38%); 62% - 78% de campos de preservación y descriptivos vacíos.	Directriz PREMIS (3.4.2); Acuerdo AGN 001 de 2024 (Art. 4.3.1.6 Descripción documental, Metadatos); OAIS (Función de Ingesta).	Pérdida de Autenticidad y Trazabilidad a largo plazo del documento, al no registrar su contexto, origen y ciclo de vida.

PARTE INTEGRAL DEL ANEXO TECNICO

Requisito (R)	Brecha Crítica del Diagnóstico (B)	Norma / Estándar de Referencia (N)	Impacto de No Cumplimiento / Riesgo Mitigado
R3. Creación de PIA (Ej. Soporte a la preservación diferenciada y asociación obligatoria de metadatos PREMIS)	Falta de Controles de Preservación: 100% de entidades carecen de Repositorios Seguros de Confianza (RSC) y no usan PREMIS/METS.	PREMIS (Diccionario de Metadatos de Preservación); OAIS (Función de Almacenamiento Seguro); NTC-ISO 16363 (Gestión de objetos digitales).	Incapacidad para demostrar la inalterabilidad del contenido y la cadena de custodia ante auditorías. Alto riesgo de pérdida de integridad semántica y estructural.
R4. Planificación de la Preservación (Ej. Integración con PRONOM para monitoreo de formatos y soporte a estrategias de migración)	Riesgo de Obsolescencia Tecnológica: Existencia de formatos de riesgo (JPEG, DOC, MP3) y obsolescencia de equipos reproductores (Beta, U-matic).	OAIS (Función de Planificación de la Preservación); Acuerdo AGN 001 de 2024 (Art. 6.1.3.2 Formulación del Plan de Preservación Digital a Largo Plazo).	Pérdida de Accesibilidad y Disponibilidad de los documentos digitales cuando sus formatos o *software* de lectura dejen de ser soportados.
R7. Acceso Seguro (PIC) (Ej. Garantía de autenticidad del PIC y trazabilidad con el PIA)	Riesgo de Pérdida de Integridad del Expediente: Fallas de interoperabilidad y fragmentación del expediente electrónico en las entidades distritales.	OAIS (Función de Acceso/Distribución); Acuerdo AGN 001 de 2024 (Art. 4.4.1 Transferencias: asegurar integridad, autenticidad, fiabilidad, inalterabilidad y disponibilidad).	Compromiso de la Autenticidad del documento entregado al usuario y riesgo legal al no poder probar la fidelidad de la copia de consulta respecto al original preservado.

PARTE INTEGRAL DEL ANEXO TÉCNICO

Requisito (R)	Brecha Crítica del Diagnóstico (B)	Norma / Estándar de Referencia (N)	Impacto de No Cumplimiento / Riesgo Mitigado
R8. Seguridad y Administración de Paquetes (Ej. Verificación periódica de integridad *hash* o *fixity*)	Inexistencia de Controles de Integridad Digital: Ninguna entidad aplica controles automáticos de integridad (checksums) sobre los documentos custodiados.	NTC-ISO 16363 (Mecanismos de verificación de integridad, Auditoría); Acuerdo AGN 001 de 2024 (Art. 4.4.1 asegurar integridad).	Corrupción Silenciosa de Datos y Pérdida Irreversible de Información sin detección oportuna. Riesgo alto de continuidad operativa.
R9. No Funcional: Arquitectura (Ej. Escalabilidad 64 bits y Arquitectura de tres capas)	Arquitectura Incipiente Distrital: La madurez tecnológica es Básica/Inicial; la infraestructura actual soporta la gestión cotidiana pero no garantiza la trazabilidad a largo plazo.	TOGAF®, UML (Estándares de Diseño y Gobernanza de Arquitectura); NTC-ISO 16363 (Capacidad de evolución tecnológica).	El sistema no soporta el volumen futuro de transferencias, limitando la sostenibilidad y escalabilidad del repositorio digital confiable.
R9. No Funcional: Trazabilidad (Ej. Pistas de auditoría inalterables que registren acciones sobre el CCD/TRD)	Falta de Trazabilidad Archivística: Ausencia de evidencia de uso sistemático de los instrumentos archivísticos (TRD/TVD/CCD) por proceso.	Acuerdo AGN 001 de 2024 (Art. 4.3.1.4 Clasificación, Art. 4.3.1.7 Conformación de unidades documentales).	Inconsistencia Archivística y riesgo legal al no poder probar la correcta aplicación de la valoración documental y disposición final de los expedientes.

PARTE INTEGRAL DEL ANEXO TÉCNICO

REFERENCIAS

Archivo General de la Nación. (2024). *Acuerdo 01 de 2024. Por el cual se compilan y actualizan los lineamientos técnicos en materia de gestión documental y preservación digital.* Bogotá, D.C.

Archivo General de Bogotá. (2025). Programa de Reprografía – PR-2025-20008. Subdirección de Gestión del Patrimonio Documental.
Archivo General de Bogotá. (2025). Sistema Integrado de Conservación – SIC-2025-20008. Subdirección de Fortalecimiento Institucional.

Archivo General de Bogotá. (2025). *Plan de Preservación Digital del Archivo General de Bogotá (Entregable 3.2.2, versión 5).* Bogotá, D.C.

Congreso de la República de Colombia. (2000). *Ley 594 de 2000. Ley General de Archivos.* Diario Oficial No. 44.093.

Congreso de la República de Colombia. (1999). *Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.* Diario Oficial No. 43.673.

Congreso de la República de Colombia. (2012). *Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.* Diario Oficial No. 48.587.

Congreso de la República de Colombia. (2014). *Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.* Diario Oficial No. 49.084.

Presidencia de la República. (2015). *Decreto 1080 de 2015. Decreto Único Reglamentario del Sector Cultura.* Diario Oficial No. 49.523.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2022). *Decreto 767 de 2022. Política de Gobierno Digital.* Diario Oficial No. 52.046.

Alcaldía Mayor de Bogotá. (2018). *Decreto Distrital 828 de 2018. Por el cual se crea el Sistema Distrital de Archivos (SDA).* Bogotá, D.C.

Consejo Nacional de Política Económica y Social. (2019). *Documento CONPES 3975 de 2019. Política Nacional de Transformación Digital e Inteligencia Artificial.* Bogotá, D.C.

Consejo Nacional de Política Económica y Social. (2020). *Documento CONPES 3995 de 2020. Política Nacional de Confianza y Seguridad Digital.* Bogotá, D.C.

International Organization for Standardization. (2024). *ISO 14721:2024 – Open Archival Information System (OAIS) Reference Model.* Geneva: ISO.

International Organization for Standardization. (2012). *ISO 16363:2012 – Audit and Certification of Trustworthy Digital Repositories.* Geneva: ISO.

International Organization for Standardization. (2009). *ISO/IEC TR 24766:2009 – Guide for requirements engineering tool capabilities.* Geneva: ISO.

PARTE INTEGRAL DEL ANEXO TÉCNICO

International Organization for Standardization. (2017). *ISO 23081-1:2017 – Information and documentation: Metadata for records.* Geneva: ISO.

Library of Congress. (2015). *PREMIS Data Dictionary for Preservation Metadata (Version 3.0).* Washington, D.C.

National Digital Stewardship Alliance. (2022). *NDSA Levels of Digital Preservation (Version 2.0).* Washington, D.C

PARTE INTEGRAL DEL ANEXO TÉCNICO