Igualdad

República de Colombia
Ministerio de Igualdad y Equidad

INSOR

Instituto Nacional para Sordos

Gustavo Francisco Petro Urrego
Presidente de la República

Francia Márquez Mina
Vicepresidenta de la República

INSTITUTO NACIONAL PARA SORDOS - INSOR
Geovani Andrés Meléndres Guerrero
Director General

Adriana Margarita Urbina
Secretaria General

Diego Armando López Cely
Subdirector de Promoción y Desarrollo

Luz Mary López Franco
Subdirectora de Gestión Educativa

Carolina Ramos Castellanos
Jefe de Oficina Asesora de Planeación y Sistemas

Estefanía Pisciotti Blanco
Jefe de Oficina Asesora Jurídica

José Fernando Duque Gallego
Asesor de la Dirección General

PLAN DE PRESERVACIÓN DIGITAL A LARGO PLAZO INSOR 2026

CONTENIDO

INTRODUCCIÓN 4
1. CONTEXTO ESTRATÉGICO INSTITUCIONAL 5
2. VISIÓN ESTRATÉGICA DE LA GESTIÓN DOCUMENTAL 9
3. DEFINICIONES 10
4. DESARROLLO DEL PLAN DE PRESERVACION DIGITAL 13
4.1. OBJETIVO GENERAL 14
4.2 OBJETIVOS ESPECÍFICOS 14
4.3 PRINCIPIOS DEL PLAN DE PRESERVACIÓN DIGITAL 14
4.4. ESTRATEGIAS DE PRESERVACIÓN DIGITAL 16
4.5 RIESGOS PARA LA PRESERVACIÓN DIGITAL A LARGO PLAZO 18
4.6 SEGURIDAD DE LA INFORMACIÓN 19
5. ADMINISTRACIÓN DE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO EN EL INSOR 22
5.1 ACTIVIDADES PREVIAS AL CARGUE DE DOCUMENTOS 25
5.2 RESPONSABLES 28
5.3 CRITERIOS PARA LA CONFORMACIÓN DE EXPEDIENTES ELECTRÓNICOS 29
5.4 EXPEDIENTE ELECTRÓNICO CONTRACTUAL 34
6. SERVIDORES Y ESPACIOS DE ALMACENAMIENTO 39
7. CRONOGRAMA DE ACTIVIDADES 42
8. HERRAMIENTAS DE SEGUIMIENTO 43

INTRODUCCIÓN

El Instituto Nacional para Sordos – INSOR, en cumplimiento de la Ley 594 de 2000 (Ley General de Archivos de Colombia), específicamente lo dispuesto en el artículo 46 sobre conservación documental, establece la obligación de implementar un sistema integrado de conservación en cada una de las fases del ciclo vital de los documentos de archivo. Este plan constituye un conjunto de acciones articuladas a corto, mediano y largo plazo, orientadas a desarrollar programas, estrategias, procesos y procedimientos que garanticen la preservación a largo plazo de los documentos electrónicos de archivo, asegurando que conserven sus atributos de autenticidad, integridad, confidencialidad, inalterabilidad, fiabilidad, interpretación, comprensión y disponibilidad a lo largo del tiempo.

De acuerdo con la normativa vigente, los sujetos obligados que generen documentos por medios electrónicos deben registrar en las Tablas de Retención Documental (TRD) los formatos electrónicos correspondientes a cada tipo documental, que conforman expedientes, series y subseries. Los documentos electrónicos de archivo deben ser gestionados conforme a los principios y procesos archivísticos, permaneciendo almacenados electrónicamente durante todo su ciclo de vida y bajo los lineamientos del Plan de Preservación Digital a Largo Plazo.

Es fundamental, desde la planeación y producción de los documentos electrónicos de archivo, incorporar mecanismos que aseguren la fiabilidad, autenticidad, integridad, veracidad e inalterabilidad durante todo el ciclo vital, previniendo el acceso no autorizado, modificaciones, traslados, ocultamientos o destrucción de la información.

El Acuerdo 001 de 2024, "Por el cual se establece el Acuerdo Único de la Función Archivística", define los criterios técnicos y jurídicos para la implementación de la gestión documental en el Estado colombiano. En particular, el título VI sobre Conservación y Preservación de Documentos, y la sección 3 relativa al Plan de Preservación Digital a Largo Plazo, establecen que junto con el Plan de Conservación Física, estos constituyen los componentes del Sistema Integrado de Conservación: uno para documentos en soporte físico o analógico y otro para documentos digitales o electrónicos.

La preservación a largo plazo de los documentos electrónicos, incluidos datos, metadatos y expedientes, debe realizarse independientemente del sistema

informático que los haya generado, tramitado o almacenado. Para ello, se deben adoptar políticas, medidas y estándares que aseguren su consulta futura y garanticen su autenticidad, integridad, accesibilidad, disponibilidad y confiabilidad, cumpliendo las directrices del Archivo General de la Nación Jorge Palacios Preciado.

La información generada, enviada, recibida o comunicada por medios electrónicos, ópticos o similares que requiera trámite o trazabilidad, debe conservarse en el mismo medio en que fue originada o recibida. Posteriormente, se debe clasificar en carpetas y subcarpetas electrónicas conforme a las Tablas de Retención Documental y registrar en el Formato Único de Inventario Documental (FUID). Los responsables de la información deben efectuar copias de seguridad y almacenarlas en las unidades de almacenamiento que disponga la Oficina Asesora de Planeación y Sistemas.

En este contexto, el presente documento da cumplimiento a las directrices del Archivo General de la Nación y a la normatividad vigente en cuanto a la administración documental, asegurando la alineación con el Sistema de Gestión de Seguridad de la Información (SGSI) de la entidad.

1. CONTEXTO ESTRATÉGICO INSTITUCIONAL

NATURALEZA JURÍDICA

Somos una entidad pública del orden nacional, adscrita al Ministerio de la Igualdad y la Equidad, que tiene como propósito fundamental promover el goce efectivo de los derechos y la inclusión de la población sorda en Colombia.

MISIÓN

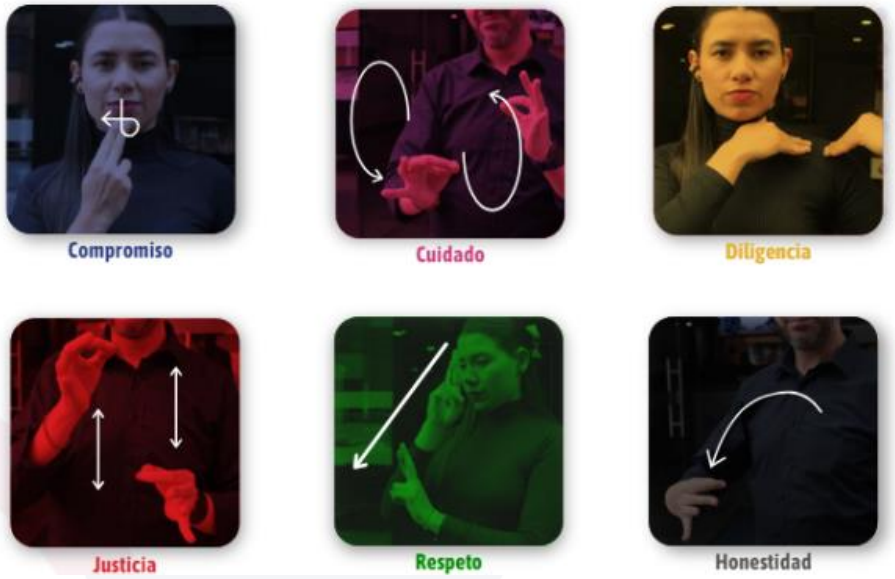
Somos la entidad pública del orden nacional que orienta y promueve la gestión e implementación de políticas públicas basadas en criterios técnicos especializados, con el propósito de contribuir a la garantía de los derechos y la equidad de oportunidades lingüísticas, sociales y culturales inclusivas de la población sorda en Colombia.

VISIÓN

En el 2026, la población sorda vivirá en un entorno más equitativo, gracias a la reducción de brechas lingüísticas, sociales y culturales, como producto de la gestión y el relacionamiento efectivo del INSOR.

VALORES DE INTEGRIDAD

Nosotros, los servidores públicos del INSOR, somos personas que con vocación y orgullo trabajamos todos los días para servir y ayudar a la población sorda colombiana. Por esta razón, adoptamos el presente código, el cual será la guía para nuestro actuar. Lo leeremos, entenderemos, sentiremos, compartiremos y aplicaremos en cada una de nuestras actuaciones del día a día. Los valores son:



Fuente: https://www.insor.gov.co/home/valores/

POLÍTICA DE CALIDAD

El Instituto Nacional para Sordos tiene como objeto promover, el desarrollo e implementación de política pública para la inclusión social de la población sorda. En virtud de ello, se compromete a destinar los recursos humanos y tecnológicos, así como la asignación adecuada y eficiente de los recursos financieros con que cuenta la entidad en cada vigencia, esto permitirá el desarrollo de su gestión con un enfoque de mejoramiento continuo, garantizando la satisfacción de sus grupos de valor, la cual es medida a través

de encuestas analizadas en la herramienta de indicadores de gestión y evidenciando así la eficacia de su sistema de gestión. Igualmente, desde la entidad se promueve el fortalecimiento y desarrollo del capital humano, a fin de lograr relaciones asertivas con los grupos de valor y ciudadanías, optimizar y promover el uso y apropiación de sus recursos físicos, tecnológicos y financieros, a afianzar la seguridad de sus activos de información y adoptar buenas prácticas para la prevención de los incidentes, accidentes, enfermedades laborales y a la protección del medio ambiente.

Para dar cumplimiento a lo anterior, se establecen los siguientes objetivos:

1. Garantizar desde la alta dirección la implementación del modelo de operación por procesos, basado en la metodología de mejora continua como el ciclo PHVA Planear, Hacer, Verificar y Actuar; comprometiéndose con la destinación de los recursos económicos, físicos y la disposición del talento humano para el cumplimiento de los objetivos institucionales.

2. Lograr un alto nivel de satisfacción de las ciudadanías y grupos de valor a través de una óptima prestación de servicios, manteniendo una relación armónica, colaborativa y de inclusión educativa y social con nuestras partes interesadas internas y externas.

3. Fomentar e incentivar espacios para generar, producir, compartir y apropiar el conocimiento tácito y explícito institucional, con el fin de ser actor orientador en materia de inclusión educativa y social de la población sorda.

4. Garantizar la administración, conservación y acceso eficiente a la información documentada producida y recibida por la entidad, a través de la aplicación de instrumentos archivísticos, estrategias de gestión documental y el uso de tecnologías de la información y las comunicaciones, con el fin de mejorar y asegurar la preservación y disponibilidad oportuna de los archivos institucionales.

5. Fortalecer la infraestructura tecnológica institucional mediante la implementación y optimización de controles de seguridad organizacionales, técnicos, físicos y legales, con el propósito de garantizar la confidencialidad, integridad y disponibilidad de la información. Para ello, se promoverá la mejora continua de herramientas de gestión, la protección integral de los activos de información y la mitigación proactiva de riesgos asociados a amenazas internas y externas en el ámbito de la seguridad digital.

6. Fomentar la protección del medio ambiente y la sostenibilidad mediante la implementación de estrategias orientadas al ahorro de energía y agua, la adecuada clasificación y disposición de residuos, así como la incorporación eficiente de tecnologías que optimicen el uso responsable de los recursos naturales. Asimismo, reducir la medición de la huella de carbono y el desarrollo de una cultura organizacional comprometida con la responsabilidad social y la mitigación del cambio climático.

7. Promover y mantener un entorno laboral seguro y saludable para todos los colaboradores de la Entidad, garantizando las condiciones de trabajo y la prevención de riesgos laborales, mediante la identificación, evaluación y control de los riesgos, así como la implementación de medidas orientadas a proteger el bienestar físico, mental y psicosocial.

8. Promover la cultura de integridad, legalidad, transparencia, buen gobierno y lucha contra la corrupción, a través de la adecuada administración de riesgos y optimización de controles, con el fin de garantizar la detección oportuna de operaciones sospechosas y la prevención eficaz de actividades ilícitas, así como prevenir y eliminar posibles actos de uso indebido del poder, de los recursos o de la información, en favor propio o para beneficios particulares.

En concordancia con los compromisos establecidos, el INSOR destinará los recursos que tenga disponibles para lograr los propósitos y objetivos mencionados, los cuales están orientados al incremento de la eficiencia, eficacia y efectividad de su desempeño institucional, dando cumplimiento a los requisitos legales y organizacionales que rigen el modelo de operación por procesos adoptado por la entidad. La política aplica a todos los procesos y está sustentada mediante la implementación del Manual de operaciones y calidad, cuyo propósito es, asegurar que cada actividad operativa contribuya directamente al cumplimiento de los objetivos y compromisos institucionales.

FUNCIONES DE LA ENTIDAD

Las funciones de la entidad se establecieron en el DECRETO NÚMERO 2106 DE 2013 "Por el cual se modifica la estructura del Instituto Nacional para Sordos" INSOR, se determinan las funciones de sus dependencias y se dictan otras disposiciones. Artículo 3. Funciones Generales. Estas son:

- Asesorar al Gobierno Nacional, Departamental y Municipal en la formulación de políticas, planes, programas y proyectos para el desarrollo integral del limitado auditivo a través de la educación.
- Promover y liderar a nivel nacional los procesos de investigación sobre la problemática de la limitación auditiva, servir de centro de información y divulgación, estadística y orientación.
- Velar por la calidad de la educación para la Población Sorda, por el cumplimiento de sus fines y por la mejor formación moral, espiritual, afectiva, intelectual y física de esta población.
- Garantizar el adecuado cubrimiento del servicio público de la educación para los limitados auditivos, con la participación de las entidades territoriales, la sociedad y la familia.
- Promover y coordinar la ejecución de planes de prevención y atención intersectoriales que permitan el desarrollo integral de los limitados auditivos.

2. VISIÓN ESTRATÉGICA DE LA GESTIÓN DOCUMENTAL

La estrategia del plan de preservación digital a largo plazo del Instituto Nacional para Sordos – INSOR se fundamenta en la implementación y apropiación de lineamientos desde la gestión documental y la función archivística, orientados a la conservación, trazabilidad y recuperación eficiente de los documentos físicos y electrónicos producidos y recibidos por la entidad. Este enfoque busca optimizar el acceso a la información, su conservación y preservación en cumplimiento de la legislación colombiana vigente.

En primera instancia, toda información generada, enviada, recibida o comunicada a través de medios electrónicos, ópticos o similares, que requiera trámite o trazabilidad, será almacenada en el mismo formato en que fue producida o recibida. Posteriormente, dicha información será organizada en carpetas y subcarpetas electrónicas conforme a las Tablas de Retención Documental, utilizando los espacios de almacenamiento institucionales (como el drive del correo institucional, carpetas compartidas en red u otros espacios determinados por la Oficina Asesora de Planeación y Sistemas) para garantizar la seguridad y conservación de la información.

El componente digital del Sistema Integrado de Conservación (SIC) se articulará con el Sistema de Gestión de Seguridad de la Información y demás sistemas administrativos de la entidad, abarcando no solo archivos digitales y electrónicos, sino también los espacios de almacenamiento, la información

publicada en las sedes electrónicas y los sistemas de información, incluyendo el Sistema de Gestión Documental Orfeo.

La estrategia se alinea con el Modelo de requisitos para la gestión de documentos electrónicos (MOREQ), asegurando que la estructura de almacenamiento responda al Cuadro de Clasificación Documental y se implemente una estructura de metadatos que facilite la producción, registro, clasificación, acceso, conservación y valoración documental a lo largo del tiempo, para garantizar la relación entre su contexto, estructura y contenido.

El acceso a los documentos electrónicos se articulará con las políticas institucionales de seguridad de la información y los lineamientos de datos abiertos, logrando un equilibrio entre transparencia y protección. Los repositorios digitales contarán con mecanismos de seguimiento, control y monitoreo, soportados en herramientas y metodologías de auditoría que aseguren su confiabilidad y fortalezcan la preservación digital a largo plazo.

Desde la Secretaría General, responsable de la gestión documental del INSOR, se establece una política clara para la administración y conservación de la información documentada, resultado de la gestión de servicios, trámites y demás procesos administrativos, tanto para usuarios internos como externos, en cumplimiento de la política pública de inclusión social de la población sorda. Esta documentación podrá conservarse en soportes análogos, electrónicos, digitales o cualquier otro medio permitido por la ley, alineándose con los diferentes sistemas de gestión vigentes en la entidad.

En conclusión, el plan de preservación digital a largo plazo se configura como una herramienta estratégica que asegura la permanencia, disponibilidad y seguridad de la memoria institucional, fortaleciendo la gestión documental y contribuyendo al cumplimiento de los objetivos misionales del INSOR, así como a la integración con otros sistemas y políticas operacionales relacionadas con la conservación y preservación de los documentos electrónicos de archivo.

3. DEFINICIONES

Accesibilidad: Capacidad de acceder al significado o al propósito esencial y auténtico de un objeto digital.

Almacenamiento de documentos: Acción de guardar sistemáticamente documentos de archivo en espacios, mobiliario y unidades de conservación apropiadas.

Archivo digital: Conjunto de acciones encaminadas a identificar, capturar, clasificar, preservar, recuperar, visualizar y dar acceso a los documentos con propósitos informativos o históricos, durante el tiempo requerido para cumplir las obligaciones legales.

Autenticidad: Garantía del carácter genuino y fidedigno de ciertos materiales digitales, es decir, que son lo que se afirma de ellos, ya sea objeto original o en tanto que copia conforme y fiable de un original, realizada mediante procesos perfectamente documentados.

Certificación: Proceso de evaluación del grado en que un programa de preservación cumple con un conjunto de normas o prácticas mínimas previamente acordadas.

Cifrado-Encriptación: Codificación de los datos según un código secreto de tal forma que sólo los usuarios autorizados puedan restablecer su forma original para consultarlos.

Comprensión: Reducción de la cantidad de datos necesarios para almacenar, transmitir y representar un objeto digital.

Conservación documental: Conjunto de medidas de conservación adoptadas para garantizar la integridad física de los documentos que alberga un archivo.

Custodia de documentos: Guarda o tenencia de documentos por parte de una institución o una persona, que implica responsabilidad jurídica en la administración y conservación de los mismos, cualquiera que sea su titularidad.

Digitalización: Técnica que permite la reproducción de información que se encuentra guardada de manera analógica (Soportes: papel, video, casettes, cinta, película, microfilm y otros) en una que sólo puede leerse o interpretarse por computador.

Documento Digital: Información representada por medio de valores numéricos diferenciados-discretos o discontinuos-, por lo general valores numéricos binarios (bits), de acuerdo con un código o convención preestablecidos.

Documento Electrónico: Es la información generada, enviada, recibida, almacenada y comunicada por medios electrónicos, ópticos o similares.

Documento Electrónico de Archivo: Registro de información generada, recibida, almacenada y comunicada por medios electrónicos, que permanece almacenada electrónicamente durante todo su ciclo de vida, producida por una personas o entidad en razón de sus actividades o funciones, que tiene valor administrativo, fiscal, legal o valor científico, histórico, técnico o

cultural y que debe ser tratada conforme a los principios y procesos archivísticos.

Elementos Esenciales: Elementos, características y atributos de un objeto digital determinado que deben preservarse para representar debidamente su significado o propósito esencial.

Estampado Cronológico: Secuencia de caracteres que indican la fecha y hora en que ocurrió un evento.

Firma Digital: Datos que cuando se adjuntan a un documento digital, permiten identificar la autenticidad e integridad.

Firma Electrónica: Métodos tales como códigos, contraseñas, datos biométricos o claves criptográficas privadas que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable, y apropiado respecto de los fines para los cuales se utiliza la firma atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente.

Formato de Archivo: codificación de un tipo de archivo que se puede obtener o interpretar de manera consistente, significativa y esperada, a través de la intervención de un software o hardware particular que ha sido diseñado para manipular ese formato.

Identidad de Objetos Digitales: Característica que permite distinguir un objeto digital del resto, incluidas otras versiones o copias del mismo contenido.

Metadatos: Datos relativos a otros datos, por lo general, muy estructurados y codificados para su procesamiento e interrogación por computadora.

Metadatos de preservación: Metadatos destinados a ayudar a la gestión de la preservación de materiales digitales documentando su identidad, características técnicas, medios de acceso, responsabilidad, historia, contexto y objetivos de preservación.

Microfilmación: Técnica que permite registrar fotográficamente documentos como pequeñas imágenes en película de alta resolución.

Migración: proceso de mover los registros, incluyendo sus características existentes, de una configuración de hardware o software a otras, sin cambiar el formato.

Preservación Digital: Es el conjunto de principios, políticas, estrategias y acciones específicas que tienen como fin asegurar la estabilidad física y tecnológica de los datos, la permanencia y el acceso de la información de los documentos digitales y proteger el contenido intelectual de los mismos por el tiempo que se considere necesario.

Protección de datos: Operaciones destinadas a resguardar los dígitos binarios que constituyen los objetos digitales de pérdidas de datos provocadas por el deterioro o el reemplazo de los medios de almacenamiento.

Refrescamiento: Proceso que consiste en copiar los datos de un soporte a otro sin cambiar su codificación, para evitar pérdidas de datos provocadas por el deterioro o el reemplazo de los medios de almacenamiento.

Reprografía: Conjunto de técnicas, como la fotografía, el fotocopiado, la microfilmación y la digitalización, que permiten copiar o duplicar documentos originalmente consignados en papel.

Sello Digital: Método para garantizar la integridad de un documento, que incluye funciones hash, firmas digitales, y, opcionalmente, estampado cronológico.

4. DESARROLLO DEL PLAN DE PRESERVACION DIGITAL

El Plan de Preservación Digital constituye el componente fundamental dentro del Sistema Integrado de Conservación, alineándose con las disposiciones y directrices institucionales que rigen la gestión documental y la conservación de documentos electrónicos en la entidad.

Política Institucional de Gestión Documental: Las estrategias de preservación y conservación de los documentos electrónicos están directamente alineadas con el Sistema de Gestión de Seguridad de la Información (SGSI) de la entidad. Esta integración busca garantizar la protección, integridad y disponibilidad de la información electrónica frente a riesgos tecnológicos y operativos.

Estructura Normalizada y Respuesta a Necesidades Específicas: El Plan se fundamenta en una estructura normalizada que responde a las necesidades específicas de preservación digital de la entidad. Considera el acceso y la disponibilidad de la información electrónica, abarcando sistemas de información, sedes electrónicas, datos abiertos y otros aspectos relevantes para los usuarios internos y externos.

Obligaciones Legales y Normativas: El cumplimiento de obligaciones legales se asegura a través de la normatividad vigente y los resultados derivados de la política de Gestión Documental. Esto incluye la medición anual a través del formulario único de avance a la gestión (FURAG) del Modelo Integrado de Planeación y Gestión (MIPG), que permite evaluar los avances y ajustes necesarios en el plan.

Limitaciones Institucionales: El Plan reconoce las limitaciones jurídicas, financieras y técnicas de la entidad, especialmente en lo referente a la

infraestructura tecnológica disponible. Estas restricciones son revisadas por el proceso de Gestión TIC de la Oficina Asesora de Planeación y Sistemas, dependencia que también lidera el SGSI en el INSOR.

Necesidades de los Usuarios: Se consideran las necesidades de los usuarios en cuanto a medios tecnológicos y capacitación, partiendo de la evaluación de la capacidad técnica de la entidad y el nivel de conocimiento de los usuarios. Esto permite orientar las acciones formativas y de soporte para el uso efectivo de los sistemas y herramientas digitales.

Buenas Prácticas, Guías y Estándares: Finalmente, el Plan incorpora las buenas prácticas establecidas al interior de la entidad, así como las guías, normas técnicas y estándares vigentes que contribuyen a la consolidación de un proceso robusto y sostenible de preservación digital.

4.1. OBJETIVO GENERAL

Fortalecer la implementación del componente digital del Sistema Integrado de Conservación en la entidad, para la conservación y preservación a largo plazo de los documentos electrónicos de archivo, alineado con el Sistema de Seguridad de la Información de la entidad.

4.2 OBJETIVOS ESPECÍFICOS

1. Actualizar y mantener el Registro de Activos de Información y el Índice de Información Clasificada y Reservada, garantizando su coherencia y alineación permanente con la Matriz de Activos de Información.
2. Elaborar el Programa de Gestión de Documentos Electrónicos de Archivo, adaptando su contenido a las necesidades específicas de la entidad para fortalecer la administración y conservación de estos documentos.
3. Sostener el indicador de cierre oportuno de radicados en Orfeo, manteniéndolo por encima del 90% al cierre de la vigencia 2026.
4. Realizar el monitoreo permanente del funcionamiento del Sistema de Información Orfeo, asegurando su óptimo desempeño y aportando eficazmente al proceso de gestión documental, mediante la creación de casos en la mesa de servicio GLPI ante la ocurrencia de cualquier novedad.
5. Incorporar los riesgos asociados a la preservación digital a largo plazo dentro de la matriz de riesgos de seguridad de la información.

4.3 PRINCIPIOS DEL PLAN DE PRESERVACIÓN DIGITAL

El Plan de preservación digital consiste en un conjunto de acciones orientadas a asegurar que los documentos generados por el Instituto conserven su integridad, autenticidad y accesibilidad durante todo el tiempo que sean necesarios y útiles para la Entidad. Para lograrlo, es fundamental aplicar los siguientes cuatro principios:

4.3.1. Principio de Planeación

La gestión de los documentos electrónicos de archivo exige una planificación cuidadosa que inicia desde su creación y se extiende hasta la decisión sobre su disposición final. Este proceso abarca etapas esenciales como la resolución de trámites, la organización archivística y el mantenimiento, todo orientado a asegurar su adecuada conservación. Es fundamental considerar desde el principio que estos documentos pueden presentarse en distintos formatos —textos, imágenes fijas, material audiovisual, sistemas de información y otros soportes—, y que todos ellos contienen información valiosa generada por diversos dispositivos.

Por lo tanto, es imprescindible que estas evidencias documentales permanezcan almacenadas durante períodos prolongados, garantizando que los registros conserven su autenticidad, integridad y fiabilidad a lo largo del tiempo que permitan su acceso y disponibilidad adecuada para los usuarios que los requieran.

4.3.2. Principio de Identificación

El Principio de Identificación debe estar en concordancia con las series y subseries definidas en la Tabla de Retención Documental, así como con los tipos documentales que establece este instrumento archivístico (TRD). La identificación se efectuará sobre el documento original que sea electrónico al momento de su archivo.

4.3.3. Principio de Nacido Digital

El documento se crea mediante procesos informáticos, por lo que su versión original es electrónico. A lo largo de su ciclo de vida, este documento permanece en su formato digital nativo, siendo gestionado, almacenado y preservado de manera electrónica.

4.3.4. Principio de Convertido Digital

Los documentos originalmente en soporte analógico son transformados a formatos digitales mediante técnicas de digitalización, lo que permite reproducir información almacenada en medios como papel, video, casetes, cintas, películas, microfilm y otros, en un formato que solo puede ser leído o interpretado por sistemas de información.

Estas copias digitales se generan principalmente para facilitar el acceso y la consulta de la información; sin embargo, no reemplazan el documento físico ni modifican los tiempos de retención establecidos en las Tablas de Retención Documental (TRD).

4.4. ESTRATEGIAS DE PRESERVACIÓN DIGITAL

Las estrategias de preservación digital son una conjugación de los principios y las alternativas técnicas y procedimentales frente a las demandas de documentos electrónicos de archivo que deben preservarse por largos periodos de tiempo. Estas estrategias son:

4.4.1 Identificar los documentos electrónicos definitivos

Es fundamental verificar la autenticidad e integridad del documento como el contar con una firma digital o un sello de tiempo válidos, así como cerciorarse de que su contenido no haya sido alterado. Además, resulta imprescindible comprobar que el documento cumple con los requisitos legales y de gestión documental establecidos por la organización.

Se entiende por registro de información aquel conjunto de datos generados, producidos, recibidos o comunicados por medios electrónicos, que permanecen almacenados digitalmente durante todo su ciclo de vida. Esta información es producida por una persona o entidad en el ejercicio de sus actividades o funciones, y posee valor administrativo, fiscal, legal, científico, histórico, técnico o cultural. Por ello, debe ser gestionada conforme a los principios y procesos archivísticos.

4.4.2. Administrar versiones de los documentos electrónicos de archivo

Las versiones son documentos electrónicos de archivos que han sufrido cambios o modificaciones, pero que formalmente han sido aceptadas con tiempos de vigencia. Es decir que cada versión es una evidencia documental electrónica, que debe ser preservada como parte del expediente que refleja el desarrollo de un trámite para contextualizar y comprender los documentos de archivo.

4.4.5. Respetar el formato original del fichero electrónico recibido

La estrategia pretende respetar el formato original para garantizar y asegurar los atributos de los documentos electrónicos de archivo. El correo electrónico (nacido digital) supondrá una radicación del documento en el formato original de llegada y realizará el circuito de vida en este formato, hasta llegar a la clasificación documental y su respectiva disposición final. Igual que ha de suceder para un documento Word o PDF, que correspondientemente se almacenará en el expediente como un documento electrónico con extensión DOC, DOCX, PDF, respectivamente.

4.4.6. Normalizar la producción electrónica de documentos

Sobre los documentos electrónicos que la institución tenga control, como los generados al interior de la entidad, deberá regular y normalizar la creación y especificar las características y atributos de generación, orientadas en el uso de estándares para la preservación a largo plazo. Por lo anterior, en el 2024 se elaboró el documento de Normalización de Formas y Formularios electrónicos de la entidad.

4.4.7. Utilizar metadatos de preservación

Los metadatos cumplen la función de proporcionar la identificación y descripción de los documentos, con lo que es posible disponer de la información necesaria para el tratamiento de los mismos. En el Sistema de Gestión Documental Orfeo de la entidad, estos metadatos hacen parte del formulario con el cual se radican las comunicaciones de entrada, internas, de salida, resoluciones y PQRS de la entidad y se evidencian en el módulo de consulta.

4.4.8. Firmar electrónicamente (avanzada o simple) con vigencia únicamente para el trámite

La firma electrónica es un conjunto de objetos y procesos, tanto internos como externos: Una clave pública y otra privada; una autoridad externa de certificación que valida ese par de claves; un proceso de conversión de un fichero a un cierto tipo de código basado en un algoritmo externo; ese algoritmo; el valor hash producido por el algoritmo; el proceso de encriptación del valor hash y la clave privada; el objeto firma resultante; el proceso de asignación de la firma al documento; el proceso de transmisión; el proceso de desencriptación; el proceso de recalcular el valor hash y de chequeo del mismo;

el certificado digital que asegura que la clave pertenece a este emisor y no a otro y la autoridad externa con capacidad para emitir estos certificados digitales.

Esta estrategia propone el uso exclusivo de firma electrónica durante el tiempo de vigencia del trámite (desde la apertura, hasta el cierre del expediente), pero su eliminación una vez concluido. Justifica que la firma tiene un grado de utilidad proporcional a la vigencia de los documentos, pero una vez terminan los trámites, pueden ser capturados los elementos de la firma como metadatos de evidencia, sin que necesariamente deban estar vigentes las certificaciones y validaciones en el documento electrónico. Para el caso de documentos con la necesidad de firmas electrónicas vigentes y activas durante largos periodos de tiempo, la estrategia propone el uso de firmas de preservación digital longevas, con recomendación de uso exclusivo para las tipologías documentales, con base en un análisis documental previo.

4.4.9. Archivar y mantener el acceso a los documentos electrónicos de archivo

Los documentos electrónicos de archivo se deben almacenar y mantener accesibles a través de políticas de seguridad. (Ver numeral 5 de este documento).

4.5 RIESGOS PARA LA PRESERVACIÓN DIGITAL A LARGO PLAZO

Los riesgos asociados a la preservación digital deben identificarse considerando los aspectos técnicos propios de los diferentes tipos de información, soportes y formatos digitales. Dada la naturaleza particular de los documentos electrónicos o digitales, es fundamental evaluar y gestionar, al menos, los siguientes riesgos mínimos al momento de formular un Plan de Preservación Digital a Largo Plazo:

- **Obsolescencia y degradación del soporte físico**. Este riesgo se refiere a la posibilidad de que los dispositivos o medios donde se almacena la información digital (como discos duros, CD, DVD, cintas magnéticas, entre otros) se deterioren con el tiempo o queden obsoletos, dificultando el acceso a los datos guardados. El desgaste físico, la falta de repuestos y la descontinuación tecnológica pueden provocar la pérdida irreversible de información.
- **Obsolescencia del formato del documento digital.** Los formatos en los que se almacenan los documentos digitales (por ejemplo, .doc, .pdf, .jpeg) pueden volverse incompatibles con los nuevos sistemas y aplicaciones. Si un formato deja de ser soportado, puede ser imposible abrir o interpretar el

contenido sin recurrir a procesos de migración o conversión, lo que pone en riesgo la integridad y accesibilidad de la información.

- **Obsolescencia del software**. El software necesario para acceder, visualizar o gestionar los documentos digitales puede dejar de actualizarse o ser descontinuado. Esto dificulta el acceso a la información, ya que los programas antiguos pueden no funcionar en sistemas modernos, generando la necesidad de mantener versiones antiguas o buscar alternativas compatibles.
- **Obsolescencia del hardware.** Los equipos físicos (computadores, lectores, servidores) utilizados para almacenar o acceder a la información digital pueden volverse obsoletos. La falta de compatibilidad con nuevas tecnologías o la imposibilidad de encontrar piezas de repuesto puede significar que los datos almacenados sean inaccesibles si no se migran oportunamente a nuevos dispositivos.
- **Desastres naturales**. Incidentes como incendios, inundaciones, terremotos o tormentas pueden dañar o destruir los sistemas de almacenamiento físico y las infraestructuras tecnológicas, ocasionando la pérdida total o parcial de la información digital si no existen copias de seguridad o planes de contingencia adecuados.
- **Ataques deliberados a la información**. Se refiere a amenazas como el hacking, malware, virus informáticos o el robo de datos, donde personas malintencionadas buscan alterar, destruir o acceder ilegalmente a la información digital. Estos ataques pueden comprometer la integridad, confidencialidad y disponibilidad de los documentos digitales.
- **Fallas organizacionales**. La ausencia de políticas claras, procedimientos deficientes, falta de capacitación del personal o errores en la gestión pueden poner en peligro la preservación a largo plazo de la información digital. Estas fallas pueden llevar a la pérdida, corrupción o inaccesibilidad de los documentos.
- **Errores humanos**. Los descuidos, equivocaciones o acciones involuntarias de las personas que manipulan la información digital pueden causar la eliminación accidental, modificación no autorizada o pérdida de datos importantes. La capacitación y la supervisión son esenciales para mitigar este riesgo.

4.6 SEGURIDAD DE LA INFORMACIÓN

La protección de documentos esenciales va más allá de las medidas habituales de protección de los documentos contra incendios, robos, inundaciones, actos de vandalismo y sustancias peligrosas, existe una serie de recursos preventivos para proteger contra catástrofes naturales y guerras.

Copias de Seguridad: Se refiere al proceso de hacer duplicados exactos del objeto digital. Aunque es un componente esencial de todas las estrategias de preservación, las copias de seguridad en sí mismas no son una técnica de mantenimiento a largo plazo, ya que se ocupa exclusivamente con la cuestión de pérdida de datos debido a un fallo de hardware, o debido a causas normales, o a desastres naturales, o a destrucción malintencionada.

En ocasiones, se combina con almacenamiento remoto de tal forma que el original y las copias no estén sujetas a los mismos eventos de desastre. Las copias de seguridad deberían ser consideradas la estrategia de mantenimiento mínima para incluso los materiales más efímeros y con menos valor que dispongamos.

Migración de la Información a otros soportes: Los procesos de conservación preventiva tanto para el original como para las reproducciones, debe normalizarse, con el fin de minimizar el riesgo de deterioro que puedan sufrir durante y después de los procesos de migración o reproducción (microfilme, fotografía, fotocopias, digitalización, etc). La estrategia debe enfocarse hacia el personal a cargo de la manipulación de los documentos en proceso reprográficos, al personal de depósito, servicios al público y a los usuarios).

Debe evaluarse previamente el estado físico y de integridad de la documentación, teniendo en cuenta sus valores administrativos e históricos para fijar prioridades y establecer las acciones de conservación durante y después del proceso de migración.

La Oficina de Planeación y Sistemas opera las herramientas Hardware y Software para la administración de la información en el Instituto. Actualmente el Instituto cuenta con los siguientes programas asociados a la administración de la información:

- **Sistema de Información Financiera –SIIF**: es una herramienta modular, transversal y transaccional, a través de la cual las entidades que hacen parte del Presupuesto General de la Nación realizan su gestión financiera pública, de manera estandarizada, segura, conforme a la norma en línea y tiempo real, que permite generar información consistente, confiable y oportuna[1].

[1] http://www.urf.gov.co/webcenter/portal/SIIFNacion/pages_home/informacingeneral

- **ORFEO**: Sistema de Gestión Documental que emplea normas técnicas y prácticas para la administración de los flujos documentales y archivísticos con el fin de garantizar la calidad de los procesos documentales dentro de una organización.

- **SOLGEIN**: Sistema de control de inventarios.

- **GLPI- MESA DE AYUDA**: Aplicación que permite la administración de requerimientos técnicos en las dependencias, para las solicitudes de los usuarios internos del Instituto.

Por otra parte, para un buen manejo del repositorio y garantizar la conservación y preservación de estos archivos, en materia de seguridad de la información es importante lo siguiente:

- Las credenciales de acceso son personales e intransferibles para cada usuario en el INSOR o fuera de éste.

- Las solicitudes de acceso deberán ser realizadas por el Coordinador o Jefe de Dependencia.
- Cada dependencia debe tener al menos un responsable de la administración de los archivos y deberá dar cuenta de la gestión de los mismos.
- Cada usuario debe controlar el bloqueo de la sesión cuando no lo esté utilizando o se aleje del puesto de trabajo.

- Evitar la fuga de información por dispositivos externos, herramientas de envío de información, correos electrónicos o en drive que no sean institucionales.

- Para los usuarios que tengan permisos de edición o eliminación, asegurarse antes de hacer cualquier actividad permanente.

- Evitar compartir información con personal externo o mediante cuentas no institucionales.
- Solo cargar documentos definitivos o publicados y no en revisión o borradores.

- No se debe cargar documentos con contraseña ni con otros controles de acceso que impidan la visualización del archivo.

- Los archivos en cualquiera de su extensión no deben llevar en su contenido hipervínculos que den acceso a páginas externas.

- El acceso por medio de VPN debe hacerse desde conexiones seguras, equipos de confianza y usuario autorizado.

- Los equipos personales que accedan a la VPN de la entidad, deberán contar con medidas de seguridad que garanticen la integridad y accesibilidad de la información.

- La información que se encuentre en este repositorio, no deberá estar alojada en el drive, ni otro medio virtual o espacios locales de los computadores.

- Dentro de los archivos a conservar en el repositorio no deberán existir instaladores, archivos ejecutables, archivos de ejecución de programas, ni cualquier otro software.

5. ADMINISTRACIÓN DE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO EN EL INSOR

El INSOR asegura la autenticidad, integridad, confidencialidad y conservación a largo plazo de los documentos electrónicos de archivo, conforme a las Tablas de Retención Documental. Además, garantiza su disponibilidad, legibilidad e interpretación, sin importar las tecnologías empleadas en su creación y almacenamiento.

La estrategia fundamental para la conservación preventiva y a largo plazo implementada por el Instituto se basa en procedimientos como la migración tecnológica. Por ello, los requisitos que el INSOR cumple para la preservación y conservación de los documentos electrónicos de archivo incluyen:

- Vinculación de cada documento electrónico de archivo a las actividades institucionales desarrolladas por el Instituto.

- Conservación simultánea de documentos de archivo en formato análogo y digital, en función de criterios jurídicos, las necesidades institucionales y el valor probatorio que la normativa vigente otorga a cada formato, como el uso de firmas digitales.
- El proceso de conservación de documentos electrónicos inicia desde el momento de su producción y se extiende hasta el cumplimiento del tiempo de retención y la disposición final establecida.
- Resguardo y mantenimiento de la accesibilidad a copias auténticas de documentos de archivo digital.
- Protección de la información y los datos personales, en estricto cumplimiento con lo dispuesto en la Ley 1273 de 2009 y la Ley 1581 de 2012.

De acuerdo a lo anterior, las características inherentes a los documentos electrónicos de archivo son:

AUTENTICIDAD: Desde el momento de producción del documento, se tiene en cuenta aspectos relacionados con el trámite o asunto al que corresponda, la identificación de los intervinientes o firmantes, la fecha de producción y de trasmisión, accesibilidad y permisos documentales. Además, las presunciones de autenticidad que para el caso de cada documento aplique según la normatividad vigente.

INTEGRIDAD: Ya que todos los documentos digitales dispuestos en el sistema de gestión documental, son en formato PDF, estos permanecen completos y protegidos de manipulación o cualquier posibilidad de cambio (versión o cambio de formato); así mismo, medidas contra la alteración o eliminación por personas no autorizadas.
En caso de requerirse un cambio a la estructura del documento electrónico, por razones plenamente justificadas y por personal debidamente autorizado, se deja evidencia de dichos cambios en el sistema de gestión documental.

SOPORTES DE ALMACENAMIENTO: Los soportes de almacenamientos que utiliza el Instituto son:

Disco compacto: Soporte digital óptico utilizado para almacenar cualquier tipo de información (audio, imágenes, videos, documentos).

Memoria USB: Es un dispositivo que utiliza una memoria flash para guardar información. Teóricamente puede retener los datos durante unos 20 años y escribirse hasta un millón de veces.

MIGRACIÓN: La migración es la transferencia periódica de materiales digitales de una configuración de hardware/software a otra o de una generación de tecnología a la siguiente, con el objetivo de que los objetos digitales sean accesibles por los sistemas informáticos existentes en cada momento, es decir, que los usuarios puedan recuperar, presentar y usar estos objetos independientemente del constante cambio de la tecnología.

La migración no solo resuelve la obsolescencia del soporte de almacenamiento, sino también la del entorno hardware/software en el que se creó el objeto digital.

INTEROPERABILIDAD: El Instituto garantiza la posibilidad de transferir y utilizar información de manera uniforme y eficiente entre sistemas de información, así como la posibilidad de interactuar e intercambiar datos.

SEGURIDAD: El sistema de Gestión Documental del Instituto mantiene los documentos digitales en un entorno seguro, de conformidad con las siguientes características:

El servidor tiene acceso restringido, con el fin de garantizar que ningún funcionario o particular ingrese.
El acceso a la aplicación para consulta, indización, radicación y digitalización se realiza con previa autenticación.
os documentos se encuentran en formato PDF que garantizan su inalterabilidad.

PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS: A través de los canales establecidos para la seguridad de la información en los sistemas de información, y específicamente en el sistema de gestión documental, se garantizan las condiciones técnicas y tecnológicas para la protección de la información y los datos. De igual forma el Instituto mediante Resolución interna 033 de 2017, reglamento el trámite de los derechos de petición, quejas, reclamos y sugerencias, a través de la cual se regulan las solicitudes de información y datos en los términos señalados en los procedimientos legales.

Por lo tanto, toda solicitud de información, debe estar respaldada mediante comunicación oficial dirigida al Instituto, la cual será respondida bajo los términos que establezca la ley.

Se deben garantizar los atributos del documento conforme los lineamientos establecidos por el Archivo General de la Nación para la gestión de documentos y expedientes electrónicos, estos son:

Autenticidad: Característica técnica que permite identificar al autor de un mensaje de datos, el cual es conservado en condiciones que permitan garantizar su integridad, para preservar la seguridad de la información que busca asegurar su validez en tiempo, forma y distribución. Así mismo, garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Fiabilidad: Que se encuentra completo y sin alteraciones.

Integridad: Característica técnica de seguridad de la información con la cual se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento asociados a la misma.

Disponibilidad: Característica de seguridad de la información que garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran asegurando su conservación durante el tiempo exigido por ley.

Por otra parte, Los documentos no podrán ser archivados en los expedientes sin que se encuentren dentro de su contenido las aprobaciones o firmas requeridas (si las hay) en cada una de las gestiones a realizar en todas sus etapas.

5.1 ACTIVIDADES PREVIAS AL CARGUE DE DOCUMENTOS

- Responder el correo enviado por el profesional de Gestión Documental con la (s) persona (s) encargadas del cargue de expedientes por cada una de las series y subseries documentales y la persona designada de la administración del repositorio para cada dependencia.

- Ubicar la información encontrada en drive, equipos de cómputo, discos externos, etc. los expedientes pertenecientes a las series y subseries documentales de la dependencia para que hagan parte del repositorio.

- Alistar la información siguiendo la TRD de cada una de las dependencias teniendo en cuenta lo siguiente:

- El formato de archivo de documento electrónico a utilizar es el PDF/A, el cual garantiza la preservación a largo plazo: los documentos que se reciban en Word o en pdf deberán convertirse a pdf.

- Los documentos en Excel con varias pestañas o bases de datos con mucha información contenida, se dejarán en esta extensión y se protegerán para que no sean modificables.

- El expediente estará compuesto únicamente por los documentos definitivos aprobados, validados o firmados (según sea el caso). Las correcciones, ajustes y demás modificaciones no harán parte del expediente ni se almacenarán en este repositorio.

- La información contenida en correos electrónico, se debe descargar como documento PDF y archivar en el expediente seguido al documento que está aprobando.

- Cuando la información sea enviada por correo electrónico en archivo comprimido como .zip, .ar, se debe descargar cada uno de los archivos que conforman el mismo.

A continuación, se presentan las extensiones de los archivos que garanticen la preservación a largo plazo de los documentos electrónicos[2].

Archivos PDF

PDF/A	Formato de archivo de documentos electrónicos para la Preservación a largo plazo.	.pdf	ISO 19005		✓
PDF/A-1	PDF/A-1 Restricciones en cuanto al uso del color, fuentes, y otros elementos.	.pdf	ISO 19005-1		✓
	PDF/A-1b (Subnivel b = Básico) Garantiza que el texto del documento se puede visualizar correctamente.				✓

Archivos Ofimáticos

Office OpenXML	Formato de procesador de textos basado en lenguaje XML abierto de Microsoft Office	.docx .xlsx .pptx	ISO/IEC 29500 ECMA-376

[2] Archivo General de la Nación. Guía para la Gestión de Documentos y Expedientes Electrónicos (borrador). En: https://www.archivogeneral.gov.co/sites/default/files/2017-08/BorradorGuiaDocumentoExpediente .pdf

De las herramientas ofimáticas, solo será permitido el cargue de documentos en Excel. Los documentos en Word y en Power Point, deberán ser guardados como pdf.

Archivos en video

JPEG 2000-Motion	Formato para la Preservación sin pérdida de vídeo en formato digital y migración de las grabaciones de vídeo analógicas obsoletos en archivos digitales	.mj2 .mjp2.	ISO 15444-4

Bases de datos

SQL	Structured Query Language, de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones en ella	.sql	ISO 9075-1		✓

Para garantizar que los expedientes se encuentren debidamente organizados y los documentos tengan los atributos explicados anteriormente y conserven su originalidad, cada una dependencia debe realizar control de calidad de la siguiente forma:

- Se debe verificar que los documentos electrónicos sean los definitivos y estén completos, sin distorsiones o imágenes borrosas.
- Si se encuentran documentos duplicados (repetidos) se debe dejar solo un original, para lo cual previamente se deberá ingresar y verificar estén completos, con firmas y permitan su acceso.
- Revisar que cada uno de los expedientes esté debidamente conformado según las TRD.
- Comunicar a la Oficina Asesora de Planeación y Sistemas las novedades que se puedan presentar en el repositorio.
- En caso de ser necesario, solicitar a Gestión Documental, acompañamiento o capacitación.

5.2 RESPONSABLES

A continuación, se presenta las responsabilidades de cada una de las dependencias y de aquellas que

Dependencias y Grupos Internos de Trabajo

- Garantizar que la información sea la que corresponda a la gestión y si se encuentra en otras plataformas externas, sea coherente.
- La información que se incluya debe ser la definitiva y no versiones anteriores.
- La información no sea modificable
- No se altere el archivo una vez sea cargado en este repositorio.
- Los documentos no deben tener imágenes borrosas o ilegibles.
- Solicitar los permisos de acceso al repositorio según su necesidad.
- Velar porque las personas que accedan a este repositorio hagan buen uso de él. (No alterar documentos, eliminar, modificar o editar sin permiso previo).
- Los expedientes digitales hacen parte del archivo de la dependencia, por lo que es responsabilidad de cada dependencia tanto consolidar la información en cada serie/subserie y tipos documentales, así como garantizar que los documentos proporcionados por servidores públicos y contratistas sean los definitivos, estén firmados y que el expediente esté completo.

Oficina Asesora de Planeación y Sistemas

- Aprovisionar espacio de acuerdo al requerimiento y disponibilidad
- Conceder de acuerdo a las solicitudes, los permisos de acceso al repositorio
- Generar copias de seguridad periódicas.

Secretaría General

- Liderar los lineamientos establecidos para la conservación de los expedientes electrónicos en el repositorio TRD INSOR.
- Junto con la Oficina Asesora de Planeación y Sistemas, definir los lineamientos para el almacenamiento y conservación de los expedientes electrónicos en este repositorio.

- Realizar el acompañamiento para el cargue de la información en cada una de las dependencias.

5.3 CRITERIOS PARA LA CONFORMACIÓN DE EXPEDIENTES ELECTRÓNICOS

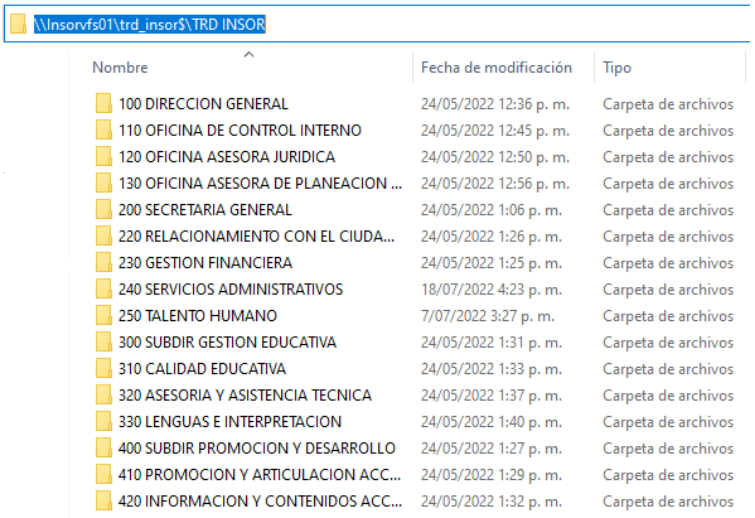
El criterio para la conformación de expedientes fue establecido en la Circular 006 de 2022, expedida por el INSOR, en cumplimiento de la Circular Externa 001 de 2020, que contiene los lineamientos para la administración de expedientes y comunicaciones oficiales. A partir de esta disposición, se desarrollaron e implementaron lineamientos específicos para la gestión de archivos digitales y electrónicos, los cuales fueron organizados y almacenados en una carpeta denominada "TRD INSOR" dentro de la infraestructura de la entidad. Esta carpeta contiene los expedientes electrónicos correspondientes al periodo 2020-2022, y su uso se ha mantenido en los años posteriores.

Los documentos incluidos en estos expedientes se organizan y almacenan de acuerdo con lo estipulado en dichos lineamientos. Estos expedientes reúnen los documentos que se producen y reciben durante la gestión administrativa de las distintas dependencias y Grupos Internos de Trabajo, clasificados según las series y subseries documentales correspondientes.

5.3.1 Ubicación

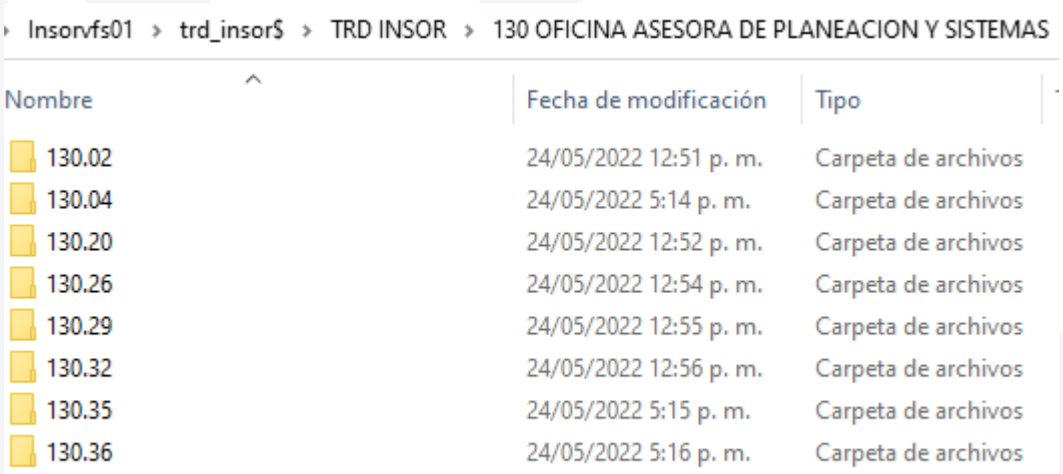
Los expedientes electrónicos se encuentran ubicados electrónicamente en la unidad de la red denominada ExpeDigital en la siguiente ruta:

\\Insorvfs01\trd_insor$\TRD INSOR



5.3.2 Estructura de las carpetas y conformación de expedientes

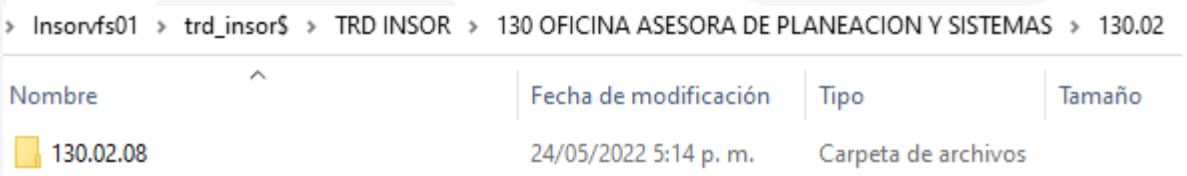
Al hacer click en cada una de las dependencias, encontrará los códigos de las series y subseries documentales, las cuales según las TRD le pertenecen. A continuación, se da el ejemplo de la Oficina Asesora de Planeación y Sistemas:



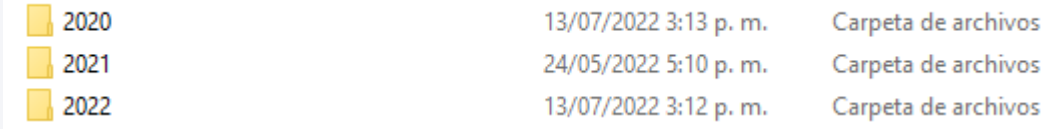
El código 130 corresponde al de la dependencia y los siguientes a las series y subseries documentales, así:

130.02 Actas
130.04 Anteproyecto de presupuesto
130.20 Informes
130.26 Manuales
130.29 Planes
130.32 Proyectos
130.35 Reporte de avance a la gestión- FURAG
130.36 Solicitud de elaboración, modificación o eliminación de documentación del sistema de gestión de calidad

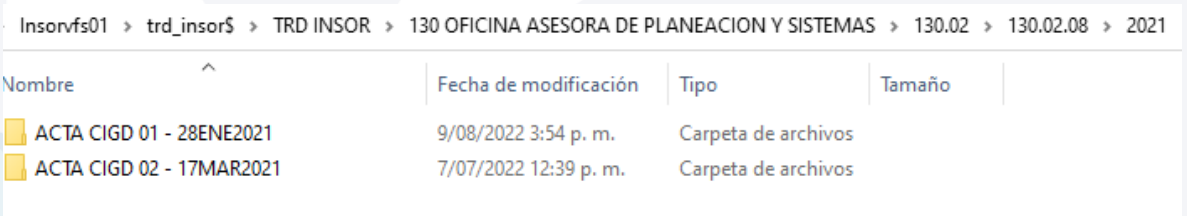
Al interior de las actas, se encuentra una subserie documental para esta dependencia:



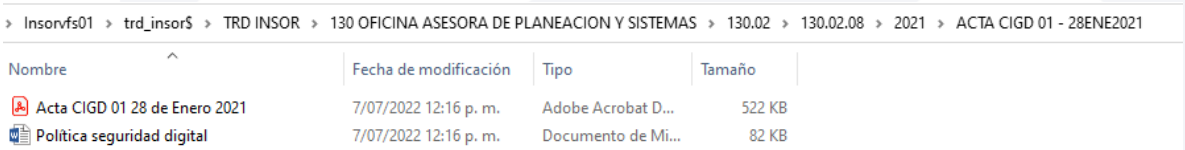
130.02.08 Actas de Comité Institucional de Gestión y Desempeño



Al interior de cada año, se colocan los expedientes que se hayan elaborado y finalizado su gestión. En este ejemplo, durante el 2021 se hicieron dos actas de este Comité, por lo que cada una de ellas se hará la marcación de la carpeta utilizando sustantivos cortos y en mayúscula, la misma denominación en los casos que se requiera y palabras claves a recordar para su acceso y consulta posterior:



Al interior de cada carpeta de expediente se colocan los archivos pdf, Excel, videos u otro tipo de documentos que lo integren.

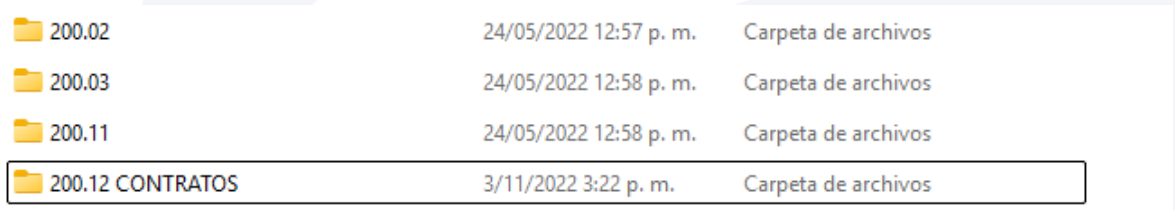


En el 2025, se ajustó la parametrización de las series y subseries, incluyendo dentro de la nomenclatura de las carpetas los nombres en cada una de ellas. Adicionalmente, la serie documental de Contratos se gestiona desde la Secretaría General, donde se realizan actualizaciones tanto de la serie como de la subserie, identificadas mediante marcación alfanumérica que incluye código y nombre. Se observa que, aunque se genera gran cantidad de información en las dependencias, esta no ha sido documentada de manera uniforme para toda la entidad, lo que limita la consolidación y trazabilidad de los registros.

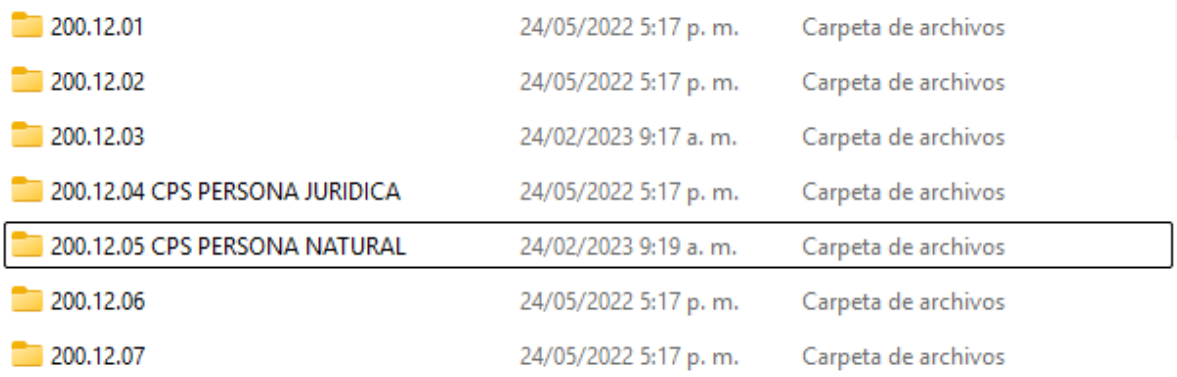
Por otra parte, El acceso, edición y lectura de las carpetas está regulado por las políticas de Seguridad de la Información, por lo que es necesario coordinar con Gestión TIC. Los expedientes forman parte del proceso de gestión contractual, siguiendo las directrices del formato de lista de chequeo, y su manejo debe estar integrado dentro del procedimiento formal. Además, se debe tener en cuenta la supervisión de la Contraloría, dado que estos documentos son auditables y deben estar disponibles en cualquier momento que se requieran. La taxonomía documental ha sido definida hasta el nivel cinco del expediente, asegurando un orden jerárquico, aunque aún se requiere avanzar en la estandarización de la nomenclatura de los archivos PDF.

Finalmente, se identificó que los nombres de los documentos, tal como aparecen en el formato de Gestión Contractual, son demasiado extensos, lo que podría provocar archivos dañados o problemas de visualización. Esto evidencia la necesidad de ajustar la marcación y establecer criterios uniformes que permitan tanto la conservación adecuada como el acceso eficiente a los documentos.

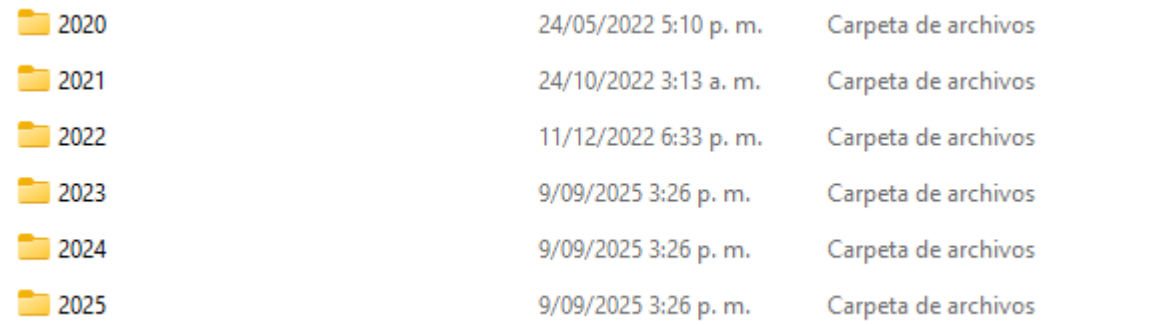
SERIE: CONTRATOS
SUBSERIE: CONTRATOS DE PRESTACIÓN DE SERVICIOS
ORDENACIÓN: Alfanumérica (códigos y nombres)
NIVEL 1: SERIE
Ejemplo: Serie



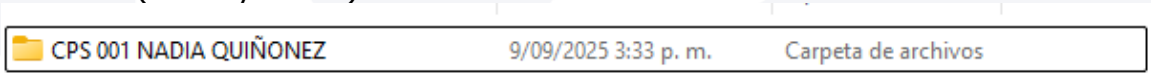
NIVEL 2: SUBSERIE
Ejemplo: Subserie:



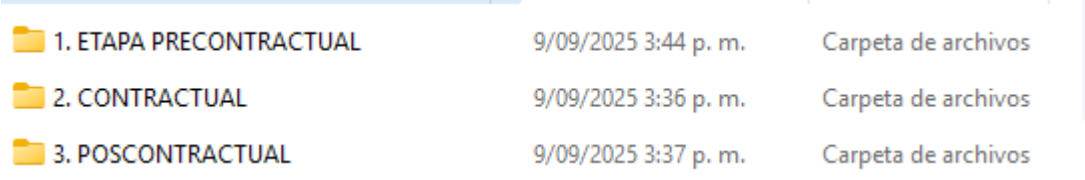
NIVEL 3: AÑO (VIGENCIA)



NIVEL 4: CPS - Número de contrato – primer nombre y primer apellido del contrato (en Mayúscula).



Nivel 5: Etapas contractuales: 1. Precontractual, 2. Contractual y 3. Poscontractual



Nivel 5.1 Documentos entidad, documentos generales y documentos Sensibles.



5.4 EXPEDIENTE ELECTRÓNICO CONTRACTUAL

Uno de los temas indispensables de la gestión documental, es el paso de expediente físico a expediente electrónico en la medida que con los avances tecnológicos, hace parte de la transformación digital en la gestión pública en Colombia. No obstante, es de anotar que antes de cualquier implementación, se debe asegurar el cumplimiento de las disposiciones establecidas en este tema desde la producción hasta la conservación en plataformas tecnológicas que permitan la disposición final.

Ahora bien, la alineación con el Plan Estratégico de Tecnología de la Información PETI es de vital importancia para asegurar que la formulación y posterior implementación se realice teniendo en cuenta los recursos e infraestructura tecnológica de la entidad, entre otros componentes requisito para esta implementación.

La gestión documental en las entidades públicas ha evolucionado significativamente con la incorporación de herramientas tecnológicas, permitiendo la transición del expediente físico al expediente electrónico. Este proceso, esencial para la transformación digital en Colombia, no solo responde a los avances tecnológicos, sino que también optimiza la administración de la información y facilita el acceso eficiente, seguro y transparente a los documentos institucionales.

Ahora bien, la implementación de expedientes electrónicos exige el cumplimiento riguroso de las normativas vigentes, garantizando que cada etapa, desde la producción hasta la conservación en plataformas tecnológicas,

se realice bajo criterios de autenticidad, integridad y preservación digital. Además, es fundamental que este proceso se alinee con el Plan Estratégico de Tecnología de la Información (PETI) de la entidad, asegurando que los recursos y la infraestructura tecnológica sean adecuados para una gestión documental efectiva y sostenible.

Por lo anterior, resulta pertinente mencionar la normativa vigente que regula los criterios para la conformación de los expedientes electrónicos. El Acuerdo 001 de 2024, expedido por el Archivo General de la Nación Jorge Palacios Preciado, establece en su Capítulo 3, titulado "Principios y criterios para el proceso de organización documental", y en la Sección 2, dedicada a los "Expedientes electrónicos", los lineamientos técnicos y jurídicos que las entidades públicas deben cumplir para su adecuada implementación.

De acuerdo con lo dispuesto en los artículos 4.3.2.2 al 4.3.2.6 del mencionado Acuerdo, los expedientes electrónicos deben conformarse atendiendo los siguientes elementos y criterios principales:

Documentos electrónicos de archivo:

Los sujetos obligados que produzcan documentos por medios electrónicos deben registrar en las Tablas de Retención Documental (TRD) los formatos electrónicos correspondientes a los tipos documentales que integran las series o subseries. Estos documentos deben ser gestionados conforme a los principios archivísticos y mantenerse almacenados electrónicamente durante todo su ciclo de vida, de acuerdo con el Plan de Preservación Digital a largo plazo. Asimismo, desde la fase de planeación y producción se deben incorporar mecanismos que garanticen la fiabilidad, autenticidad, integridad, veracidad e inalterabilidad de los documentos.

Índice electrónico

Las entidades deben implementar mecanismos tecnológicos que permitan llevar un índice electrónico de los expedientes electrónicos, el cual asegure:

- La identificación de todos los documentos que los conforman.
- La conservación del orden original definido para cada serie documental.
- La integridad del expediente durante todo su ciclo de vida.
- La actualización automática del índice con cada incorporación de documentos, garantizando autenticidad e inalterabilidad.

- La recuperación eficiente de los documentos y sus metadatos.

Firma y cierre del expediente electrónico:

Una vez finalizada la actuación o procedimiento administrativo, el funcionario autorizado deberá cerrar el expediente y firmar el índice electrónico, utilizando mecanismos seguros e interoperables que aseguren su autenticidad e integridad.

Eliminación de documentos y expedientes electrónicos

Los expedientes que hayan cumplido sus tiempos de retención y no sean objeto de conservación permanente deberán eliminarse mediante procedimientos de borrado seguro, conforme a lo establecido en las TRD y los lineamientos del Archivo General de la Nación.

Preservación a largo plazo

Los documentos y expedientes electrónicos deben conservarse garantizando su autenticidad, integridad, inalterabilidad, fiabilidad y disponibilidad, conforme a lo previsto en el Título 6 "Conservación y preservación" del Acuerdo 001 de 2024 y en el Plan de Preservación Digital a largo plazo. De este último punto, El Título 6, Sección 3 del Acuerdo 001 de 2024 establece los lineamientos para que los sujetos obligados aseguren la conservación, autenticidad, integridad, disponibilidad y accesibilidad de los documentos electrónicos a lo largo del tiempo mediante un Plan de Preservación Digital a Largo Plazo.

Responsabilidad institucional

- Los sujetos obligados son responsables de preservar todos los documentos, datos, metadatos y expedientes electrónicos, sin importar el sistema donde se generen o almacenen.
- Deben garantizar autenticidad, integridad, accesibilidad y confiabilidad de los documentos según las directrices del Archivo General de la Nación.

Criterios de preservación digital

- Identificación y mapeo de flujos de información: procesos que generan y reciben información, responsables, formatos, interdependencias y riesgos.

- Caracterización de documentos electrónicos a preservar.
- Evaluación de estrategias de preservación.
- Cumplimiento de tiempos de retención (TRD/TVD).
- Garantía de interoperabilidad, recuperación y protección de los documentos.

Gestión de riesgos

Identificación de riesgos como obsolescencia de soportes, formatos, software o hardware, desastres naturales, ataques deliberados, fallas organizacionales o errores humanos.

Estrategias de preservación digital

- Migración: traslado a nuevas plataformas o medios.
- Conversión: cambio de formato para preservación o consulta.
- Emulación: recreación de entornos tecnológicos para formatos obsoletos.
- Refreshing: transferencia de datos a nuevos soportes sin modificar contenido.

Las estrategias deben documentarse, justificarse y registrarse históricamente, incluyendo esquemas de metadatos y modelos conceptuales.

Procesos y procedimientos

- Garantizan la cadena de preservación durante todo el ciclo de vida de los documentos.
- Consideran documentos digitalizados y nativos digitales, cronogramas de transferencia y eliminación, formatos y medios de almacenamiento, metadatos, autenticidad y fiabilidad, requisitos legales, auditoría y vigilancia tecnológica.

Qué se requiere en el INSOR

Para la conformación del expediente electrónico, las Tablas de Retención Documental (TRD) vigentes establecen que la serie Contratos cuenta con soporte físico y electrónico. En caso de requerirse la conformación totalmente electrónica de esta serie, la entidad deberá implementar los criterios de preservación digital, iniciando con la identificación y mapeo de los flujos de información asociados a los procesos que conforman los expedientes

contractuales, los responsables, los formatos utilizados, la interacción entre dependencias y los riesgos vinculados, con el fin de automatizarlos en el Sistema de Información Orfeo o en otra plataforma tecnológica.

Asimismo, el sistema seleccionado debe ser interoperable con otros sistemas institucionales, y permitir la recuperación, protección e integridad de los expedientes contractuales durante todo su ciclo de vida, conforme a los tiempos de retención y disposición final establecidos en la TRD.

Actualmente, los documentos se producen en el Sistema de Información Orfeo, en el cual los radicados asociados a los contratos no se encuentran agrupados dentro de un expediente electrónico. Este sistema no cuenta con un índice electrónico ni con firmas digitales o electrónicas, ni con mecanismos que garanticen plenamente la autenticidad, integridad, accesibilidad y confiabilidad de los documentos durante todo su ciclo vital, hasta su disposición final, ya sea eliminación o preservación permanente. Estas garantías deben aplicarse a todos los documentos, datos, metadatos y expedientes electrónicos, sin importar el sistema donde se generen o almacenen.

En cuanto a los contratos, la TRD establece un tiempo de retención de dos (2) años en el archivo de gestión, contados a partir del cierre del expediente, y veinte (20) años en el archivo central antes de su disposición final mediante selección. Esto implica que, una vez cumplido el tiempo en el archivo de gestión, el Sistema de Información Orfeo o el repositorio que se utilice debe contar con un índice electrónico que permita realizar la transferencia primaria digital al Archivo Central. En este almacenamiento, la entidad deberá garantizar la conservación de los documentos por veinte años, antes de decidir si se destinan a preservación histórica o a eliminación definitiva mediante borrado seguro. Durante este proceso, también podrán realizarse transferencias documentales digitales secundarias, las cuales deberán cumplir con los requisitos técnicos y normativos establecidos.

Para los expedientes contractuales electrónicos cuya disposición final sea la preservación histórica, el INSOR deberá adoptar e implementar estrategias de preservación digital que aseguren la continuidad, accesibilidad y autenticidad de los documentos a lo largo del tiempo, evitando riesgos derivados de la obsolescencia de soportes, formatos, software o hardware. Entre estas estrategias se incluyen la migración (traslado de la información a nuevas plataformas o medios tecnológicos), la conversión (cambio de formato con fines de preservación o consulta), la emulación (recreación de entornos tecnológicos

antiguos para lectura de formatos obsoletos) y el refreshing (transferencia periódica de datos a nuevos soportes sin alterar su contenido).
Todas las acciones de preservación deben estar documentadas, justificadas y registradas, incorporando esquemas de metadatos y modelos conceptuales que garanticen la trazabilidad y fiabilidad del proceso.

En caso de avanzar en la automatización de los expedientes contractuales dentro del Sistema Orfeo o en otro sistema, se deberá asegurar la cadena de preservación digital durante todo el ciclo de vida de los documentos, parametrizando en el sistema la identificación de documentos digitalizados y nativos digitales, los cronogramas de transferencias y eliminación, los formatos y medios de almacenamiento, los metadatos y los mecanismos que garanticen la autenticidad, fiabilidad, cumplimiento normativo, auditoría y vigilancia tecnológica.

En conclusión, y conforme a lo expuesto anteriormente, actualmente la transición de los expedientes contractuales desde el formato físico hacia el electrónico debe realizarse de manera progresiva. Este proceso escalonado es fundamental para asegurar la continuidad, accesibilidad y autenticidad de los documentos, mientras la entidad implementa las mejoras tecnológicas y archivísticas necesarias que permitan una gestión electrónica integral adecuada.

6. SERVIDORES Y ESPACIOS DE ALMACENAMIENTO

OFICINA DE PLANEACIÓN Y SISTEMAS

En esta oficina se encuentra la administración de los servidores y demás medios de almacenamiento digitales a los cuales accede

UNIDAD DATA 1

- **TRD INSOR 132 GIGAS** 75.256 Archivos 21.210 carpetas
- OAPS 85 MEGAS 270 ARCHIVOS 73 CARPETAS contratos oficina planeación
- MESA DE DATOS 5.93 GIGAS 188 archivos 88 carpetas, Power BI Cristhiam Ruiz, Oscar Zapata y Angélica Betancourt
- INSOR: Historial de imágenes del papel de tapiz del directorio activo TIC 5,47 GIGAS 253 ARCHIVOS, 13 CARPETAS
- DATA EPS: Información que enviaron EPS 2021 y 2022 para el tema de niños Dirección General 55 megas 129 archivos 36 carpetas
- DATA DIG: Compartida a Angélica Betancourt no se guardó información. Ya no está e la entidad

- BKP_SYS_STATE Copia de seguridad de los servidores principales 33 Gigas, 24 archivos, 5 carpetas. Solo acceso por parte de equipo TIC
- BKP_FINALES 54 Archivos, 65 carpetas, 408 GB copias finales de servidores que ya no están en uso.
- ARCHIVO CENTRAL INSOR , 537 MEGAS 59 ARCHIVOS 14 CARPETAS

UNIDAD DATA 2

- Copia de respaldo DATA INSOR USUARIOS (f:) almacenada en servidor de toda la entidad. 1,67 TERAS en uso y 229 Gigas libres.

Nota: (Susceptible de depuración con las dependencias)

UNIDAD FS_COM

- **Usado 463 gigas y disponible 607 gigas de un total de 1,04 TERAS** carpeta 2019-2022 ORGANIZADOS. Tiene parte de Backup y de gestión para Comunicaciones e intérpretes de la Dirección General. Está en uso.

DATA _SPD (G:) TOTAL 1 TERA en uso 324 GIGAS. carpeta para el almacenamiento de información de la Subdirección de Promoción y Desarrollo, Está estructurada por años 324 GIGAS 5.459 archivos 760 carpetas

FILE SERVER 2 Tamaño 2,6 Teras

- **DISCO LOCAL total 107 gigas en uso 72 y disponible 35,1**

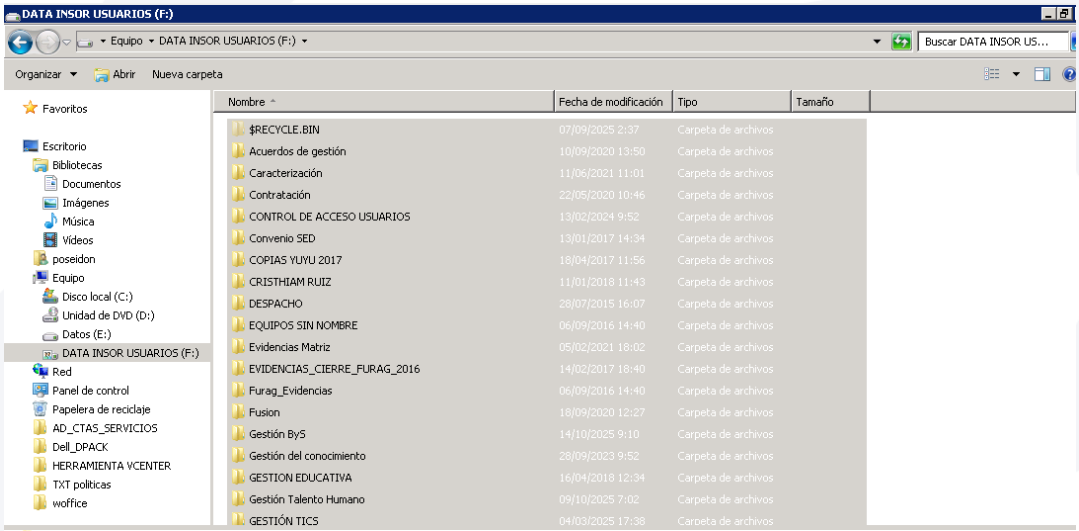
Sistema operativo del servidor administrado por equipo TIC.

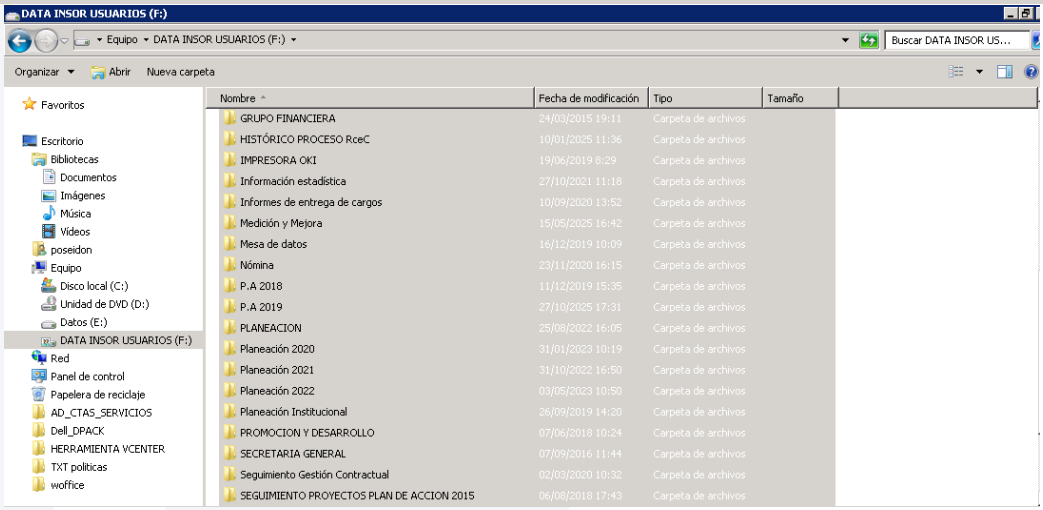
- **DATOS (E:) TOTAL 458 GIGAS en uso 360 disponibles 98 gigas**

Contiene carpetas de gestión de las áreas a partir del 2012 y se evidencia el uso de la carpeta Comisiones, pero otras se encuentran vacías o que por las fechas de última modificación fueron hasta el año 2022 o años anteriores. Dentro de ellas **INSOR DATOS** en la cual se tiene la información de la entidad por dependencias desde el 2012 hasta el 2022. Susceptible de depuración.
El acceso a esa carpeta es por dependencia.

- **DATA INSOR USUARIOS (F). 1,86 TERAS Utilizadas 1,78 Teras disponibles 84 gigas**

Contiene el Archivo de Gestión por temas diferentes para un total de 43 carpetas de todas las dependencias a partir de 2015 en adelante:





DRIVE INSTITUCIONAL

Espacio de almacenamiento tanto en correo como en drive del INSOR 39 TB a partir del 2020 a la fecha. Cuentas de correo: 205.
El contrato está vigente hasta el 10 de abril de 2026 mediante el proveedor Magos del Cloud, Orden de compra por Acuerdo Marco de Precio. Se tiene google a partir de 2020, anterior a este año se tenía sistemas de almacenamiento en nube (drive)

SERVIDORES DE APLICACIONES

- **Server App Orfeo**

300 gigas (Aplicación)
Almacenamiento bases de datos. 2 discos disco 1 50 gigas y disco 2 100 gigas
A partir de 2018

- **Serve ITS**

Aplicación: Disco de 500 gigas
Base de datos: 500 gigas
A partir 2008 (aproximadamente)

- **Server BDAlmacen (Solgein)**

Almacenamiento base de datos 200 gigas

- **SEDE ELECTRÓNICA: (INCLUYE INSOR LAB)**

Almacenamiento: Disco 1 300 gigas Disco 2 200 GB
Última actualización 2019

- **INSOR EDUCATIVO (2021)**

Almacenamiento 60 gigas

- **GLPI**

150 gigas almacenamiento

7. CRONOGRAMA DE ACTIVIDADES

N.	ACTIVIDADES	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
1	Verificar la disponibilidad y estructura de los expedientes en el Sistema de Información Orfeo para la implementación del expediente electrónico contractual en dicha plataforma.												
2	Elaborar documento identificación de procedimientos a sistematizar en el Sistema de Información Orfeo.												
3	Revisar y actualizar el análisis de contexto del proceso de Gestión Documental.												
4	Actualizar el mapa de riesgos del proceso de Gestión Documental - asociados a seguridad de la información												

5	Elaborar una propuesta de automatización procedimiento en Sistema de Información Orfeo.													
6	Elaborar el inventario documental en formato FUID para los documentos de archivo físicos o electrónicos de la Secretaría General - Gestión documental													
7	Hacer seguimiento de elaboración inventarios de Archivos de Gestión en las dependencias en formato FUID													
8	Realizar el inventario de bases de datos, desarrollos y sistemas de información.													
9	Realizar el inventario de activos de información incluyendo las bases de datos, desarrollos y sistemas de información y recurso humano													

8. HERRAMIENTAS DE SEGUIMIENTO

El seguimiento y control deben estar alineados con los requisitos impuestos por los entes de control descritos a continuación:

- Plan de acción para la Gestión Documental: Este instrumento establece las actividades, metas y responsables para la correcta administración de los documentos electrónicos de archivo. Permite realizar revisiones periódicas de los avances y ajustar estrategias según las necesidades detectadas durante el proceso.

- Resultados de la medición de la política de Gestión Documental (FURAG): Corresponde a la evaluación periódica que realiza el Formulario Único de Reporte de Avance de la Gestión (FURAG), el cual mide el nivel de cumplimiento de la política de gestión documental. Los resultados

obtenidos se utilizan para identificar fortalezas y oportunidades de mejora en los procesos, facilitando la toma de decisiones fundamentadas.

Igualdad

República de Colombia
Ministerio de Igualdad y Equidad
INSOR
Instituto Nacional para Sordos

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