

 POLITÉCNICO COLOMBIANO JAIME ISAZA CADAVID	<b>PLAN DE PRESERVACION DIGITAL</b>	<b>Código: ANL04</b>
		<b>Versión: 2</b>

## **PLAN DE PRESERVACIÓN A LARGO PLAZO**

**POLITÉCNICO COLOMBIANO JAIME ISAZA CADAVID**

**MEDELLÍN**

**2026**

 POLITÉCNICO COLOMBIANO JAIME ESCOBAR OSPINA	<b>PLAN DE PRESERVACION DIGITAL</b>	Código: ANL04
		Versión: 2

**Rector**

Jhon Alexander Osorio Saraz

[rectoria@elpoli.edu.co](mailto:rectoria@elpoli.edu.co)

Secretario General

Rodrigo Orlando Osorio Montoya

[sgeneral@elpoli.edu.co](mailto:sgeneral@elpoli.edu.co)

Coordinadora del Área de Archivo y Correspondencia

Blanca Ludivia Vargas Vargas

[archivo@elpoli.edu.co](mailto:archivo@elpoli.edu.co)

**Sedes**

**Sede Medellín**

El Poblado Teléfono: 444 76 54 Centro Regional Urabá Vereda El Reposo

Teléfono: 829 68 56

**Centro Regional Oriente Dirección:**

Calle 41 50 A 324

Teléfono: 561 51 78

**Centro de Laboratorios, Prácticas y Experimentación**

Carrera 58 No. 27 B – 125 Bello

Tel: 604 452 09 99

[claboratorios@elpoli.edu.co](mailto:claboratorios@elpoli.edu.co)

**Centro de Laboratorios de Riegos y Maquinaria Agrícola**

Diagonal 49 A No. 32 – 121 Niquía

Tel: 604 482 60 07

[claboratorios@elpoli.edu.co](mailto:claboratorios@elpoli.edu.co)

**Granja Román Gómez Gómez**

Marinilla

Tel: 604 548 58 43

[granjas@elpoli.edu.co](mailto:granjas@elpoli.edu.co)

**Granja John Jairo González Torres**

Centro de Producción y Experimentación Acuícola

San Jerónimo

Tel: 604 858 25 55

[granjas@elpoli.edu.co](mailto:granjas@elpoli.edu.co)

	<b>PLAN DE PRESERVACION DIGITAL</b>	<b>Código: ANL04</b>
		<b>Versión: 2</b>

## TABLA DE CONTENIDO

1. INTRODUCCIÓN .....	5
2. DEFINICIÓN DEL PLAN DE PRESERVACIÓN DIGITAL.....	6
3. PREREQUISITOS PARA LA FORMULACIÓN DEL PLAN DE PRESERVACIÓN DIGITAL -PPD- .....	7
3.1. ANALISIS DEL CONTEXTO INSTITUCIONAL .....	7
3.2. ANÁLISIS DE REFERENTES NORMATIVOS .....	12
4. FASES PARA LA ELABORACIÓN DEL PLAN DE PRESERVACIÓN DIGITAL -PPD- .....	13
4.1. Fase 1 Bases del PPD.....	13
4.1.1. Objetivos.....	13
4.1.2. Alcance .....	14
4.1.3. Articulación con los programas institucionales.....	14
4.1.4. Roles y responsabilidades.....	16
4.2. Fase 2 Diagnóstico.....	18
4.2.1. Identificación de documentos electrónicos a preservar.....	18
4.2.2. Diagnóstico de los documentos electrónicos a preservar .....	22
4.2.3. Análisis de riesgos .....	24
4.2.4. Evaluación de la capacidad de preservación digital en la entidad.....	29
4.3. Fase 3 Evaluación de Estrategias .....	32
4.3.1. Evaluación y selección de prioridades.....	32
4.3.1.1. Ingresar Actualizar en Sistemas de Información .....	32
4.3.1.2. Consultar en Sistemas de Información.....	33
4.3.1.3. Respalda Información .....	33
4.3.1.4. Realizar mantenimiento .....	34
4.3.1.5. Gestionar obsolescencia tecnológica.....	34
4.3.1.6. Efectuar pruebas de seguridad.....	35
4.3.1.7. Adquirir tecnología – Planeación.....	35

	<b>PLAN DE PRESERVACION DIGITAL</b>	<b>Código: ANL04</b>
		<b>Versión: 2</b>

4.3.2.	Caracterización de los documentos electrónicos a preservar .....	36
4.3.3.	Identificación y evaluación de estrategias de preservación.....	36
4.3.4.	Estrategias de preservación .....	37
4.3.4.1.	Normalización de formatos .....	37
4.3.4.2.	Migración .....	39
4.3.4.3.	Conversión .....	40
4.3.4.4.	Refreshing .....	42
4.3.4.5.	Emulación .....	43
4.3.4.6.	Características mínimas de una plataforma de preservación digital ..	44
4.3.5.	Evaluación de las estrategias de preservación.....	45
4.3.6.	Borrado Digital Seguro.....	48
4.3.6.1.	Eliminación Lógica .....	49
4.3.6.2.	Definición y Principios Fundamentales del Borrado Digital Seguro.	49
4.3.6.3.	Riesgos de una Gestión Inadecuada de Datos.....	50
4.3.6.4.	Casos de Uso Críticos para el Borrado Digital Seguro .....	50
4.3.6.5.	Métodos Lógicos (Basados en Software).....	51
4.3.6.6.	Métodos Físicos (Basados en Hardware).....	51
4.4.	Fase 4 Plan de Acción.....	53
4.4.1.	Definición de Acciones y Estrategias.....	53
4.4.2.	Definición de recursos y cronograma de ejecución.....	53
4.4.3.	Implementación del Plan de Preservación Digital.....	56
5.	MONITOREO DEL PLAN DE PRESERVACIÓN DIGITAL -PPD- .....	57
	REFERENCIAS BIBLIOGRÁFICAS .....	60

 <p>POLITÉCNICO COLOMBIANO JAIME ESCALA CADAVID</p>	<p><b>PLAN DE PRESERVACION DIGITAL</b></p>	<p><b>Código: ANL04</b></p> <hr/> <p><b>Versión: 2</b></p>
---	--	--

## 1. INTRODUCCIÓN

En un mundo dominado por lo digital, los archivos institucionales están saturados de documentos electrónicos lo que hace necesario definir estrategias y políticas no solo para su organización y control, sino también para su preservación a largo plazo para garantizar que no se pierda la información histórica para la institución sino también para la sociedad.

La preservación digital a largo plazo es un campo relativamente nuevo, pero realmente sus inicios datan prácticamente desde los inicios de la historia de la humanidad como sociedad, enmarcada en una constante búsqueda por preservar la información y el conocimiento a través de los siglos.

Los Primeros Intentos de Preservación surgen con la “Escritura” que fue un primer paso crucial en la preservación de la información, permitiendo a las civilizaciones antiguas transmitir conocimiento a través de generaciones, para ello fue necesario contar con materiales duraderos utilizados tales como el papiro, el pergamino y el papel para crear documentos que perduraran. Posteriormente fue necesario organizar y controlar esa información y surgieron las Bibliotecas y Archivos como espacios dedicados a la conservación y organización de la información.

En esta Era Digital nos enfrentamos a nuevos desafíos. Con la llegada de los computadores, la información comenzó a almacenarse en formatos digitales, lo que trajo consigo nuevos desafíos para su preservación, así como nuevos retos tales como la obsolescencia tecnológica por la rápida evolución de las tecnologías digitales lo que ha hecho que los formatos de archivo se vuelvan obsoletos con rapidez, dificultando la lectura y conservación de archivos antiguos en el tiempo, adicionalmente, los soportes digitales son más vulnerables a desastres naturales y ciberataques que los soportes físicos.

Fue así como surgió la Preservación Digital como disciplina, puesto que a medida que la dependencia de los formatos digitales se incrementaba, se hizo evidente la necesidad de desarrollar estrategias para garantizar la preservación a largo plazo de la información generada en medio digital, para lo cual se comenzaron a desarrollar estándares y normativas internacionales para la preservación digital, con el objetivo de asegurar la interoperabilidad y la longevidad de los archivos digitales, surgieron diversas herramientas y tecnologías para la migración de datos, la emulación de software y la creación de repositorios digitales, surgieron diversas herramientas y tecnologías para la migración de datos, la emulación de software y la creación de repositorios digitales.

En un entorno digital en constante evolución, la preservación digital a largo plazo de los documentos electrónicos se ha convertido en una necesidad y prioridad

 <p>POLITÉCNICO COLOMBIANO JAIME ISAZA CADAVID</p>	<p><b>PLAN DE PRESERVACION DIGITAL</b></p>	<p><b>Código: ANL04</b></p>
		<p><b>Versión: 2</b></p>

estratégica para el Politécnico Colombiano Jaime Isaza Cadavid. Este plan tiene como objetivo establecer un marco de trabajo sólido para garantizar la integridad, autenticidad y accesibilidad de la información digital a lo largo del tiempo, cumpliendo con los requisitos legales y normativos vigentes.

La preservación digital es fundamental para asegurar la continuidad de las operaciones de la Institución, proteger el patrimonio documental de la organización y facilitar el acceso a la información tanto para las partes interesadas como para las generaciones futuras. Este plan aborda los desafíos asociados a la obsolescencia tecnológica, la heterogeneidad de los formatos digitales y la gestión de grandes volúmenes de datos. A través de una combinación de medidas técnicas y administrativas, se busca garantizar la supervivencia de la información digital del Poli en un entorno digital en constante cambio.

## **2. DEFINICIÓN DEL PLAN DE PRESERVACIÓN DIGITAL**

La Preservación Digital se define como *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*<sup>1</sup>.

La Preservación Digital se aplica a los documentos electrónicos de archivo cuyo medio o formato sea digital y se ejecuta en cualquier etapa del ciclo vital del documento, de tal forma que hace parte de los procesos de la gestión documental definidos en el Decreto 1080 de 2015, específicamente el proceso de preservación digital a largo plazo y es necesario instaurar acciones desde el proceso de planeación de la gestión documental hasta la disposición final de los documentos, por lo tanto, al igual que la valoración, la preservación digital a largo plazo se considera un proceso transversal en la gestión documental, tal como se muestra en la siguiente imagen:

---

<sup>1</sup> Definición tomada del Acuerdo 06 de 2014 del AGN.

	<b>PLAN DE PRESERVACION DIGITAL</b>	<b>Código: ANL04</b>
		<b>Versión: 2</b>

**Ilustración 2-1 Procesos de la Gestión Documental<sup>2</sup>**



### 3. PRERQUISITOS PARA LA FORMULACIÓN DEL PLAN DE PRESERVACIÓN DIGITAL -PPD-

#### 3.1. ANALISIS DEL CONTEXTO INSTITUCIONAL

A continuación, se presentan elementos claves del contexto estratégico del Politécnico Colombiano Jaime Isaza Cadavid:

##### **Misión Institucional:**

Somos una Institución de educación superior estatal de vocación tecnológica, que con su talento humano ofrece una formación integral con programas de calidad en pregrado y posgrado, apoyados en la gestión del conocimiento de base científica; promovemos acciones innovadoras desde la investigación y la proyección social, para contribuir al desarrollo económico, social y ambiental de Antioquia y Colombia.

<sup>2</sup> Imagen tomada del documento “Fundamentos de Preservación Digital a Largo Plazo”

 <p>POLITÉCNICO COLOMBIANO JAIME ISAZA CADAVID</p>	<p><b>PLAN DE PRESERVACION DIGITAL</b></p>	<p><b>Código: ANL04</b></p> <hr/> <p><b>Versión: 2</b></p>
--	--	--

**Visión Institucional:**

El Politécnico Colombiano Jaime Isaza Cadavid, siempre será reconocido como una institución de alta calidad académica con énfasis en la formación y gestión tecnológica, la investigación aplicada y la proyección social, en beneficio del desarrollo económico, social y ambiental, con presencia en las regiones de Antioquia y el País; articulado a las dinámicas del sector productivo, a la política pública y al crecimiento de la cobertura en educación.

**Valores Institucionales:**

**Compromiso:** Encarar las actuaciones institucionales con el propósito de generar siempre los mejores resultados. Promover el sentido de pertenencia sobre los bienes de la Institución y las actividades académicas, culturales, pedagógicas, sociales y deportivas que se realicen dentro de ella.

**Servicio:** Atender el conjunto de actividades que buscan responder a necesidades formuladas por nuestros clientes. En este sentido, cumplir a cabalidad con los deberes encomendados para la prestación de los servicios y evitar cualquier acto que pretenda la suspensión de la prestación de estos de una manera injustificada.

**Colaboración:** Apoyar el trabajo de todos los compañeros de la Institución, en términos de cooperación y coordinación, con el fin de contribuir con el crecimiento de la comunidad politécnica resaltando la Institución como centro de formación integral.

**Imparcialidad:** Actuar siempre en forma equitativa, sin conceder preferencias o privilegios indebidos a persona alguna.

**Responsabilidad:** Cumplir con las normas y deberes de la Institución, asumiendo con entereza y reflexión sus posibles consecuencias.

**Bien Común:** En las actuaciones se debe respetar el patrimonio de la Institución, primando el interés colectivo sobre los intereses particulares.

 <p>POLITÉCNICO COLOMBIANO JAIME ESCALA CADAVID</p>	<p><b>PLAN DE PRESERVACION DIGITAL</b></p>	<p><b>Código: ANL04</b></p> <hr/> <p><b>Versión: 2</b></p>
---	--	--

Respeto: Reconocer las virtudes, derechos y libertades que son inherentes a toda persona, con trato amable y tolerante para toda la comunidad politécnica.

Liderazgo: Promover acciones que despierten las capacidades innatas y /o fortalezcan las aptitudes de los estudiantes para que sean portadores de cambio personal, familiar, profesional y social.

**Principios Institucionales:**

Responsabilidad social: Instituye la responsabilidad social para el cumplimiento de su Misión y Visión, teniendo en cuenta que responde ante la sociedad mediante sus órganos de gobierno.

Excelencia académica: Encamina su labor hacia la consecución de niveles de excelencia, para lo cual no escatimará esfuerzos que lo conduzcan a obtener logros cada vez mayores en los procesos académicos.

Innovación: Dada su vocación técnica y tecnológica, la Institución apoya y fomenta actividades conducentes a la innovación, en los campos que tengan que ver con el ejercicio de la docencia, la investigación y la extensión, con el fin de contribuir de manera eficiente y constante al desarrollo local, regional y del país.

Equidad: Se compromete a llevar a cabo sus actuaciones con justicia, buscando el beneficio educativo de todos.

Universalidad: Orienta sus procesos de docencia, extensión, proyección social e investigación, hacia la búsqueda de diversidad de campos del conocimiento y hacia el impulso del saber, mediante las relaciones entre campos especializados de la ciencia y la tecnología.

Solidaridad: Impulsa las relaciones interpersonales basadas en la dignidad humana, estrategias de crecimiento y de sensibilidad social, para el beneficio común.

Sentido de ciudadanía: Expresado mediante la creación de espacios de convivencia que faciliten la

 <p>POLITÉCNICO COLOMBIANO JAIME ESCALA CADAVID</p>	<p><b>PLAN DE PRESERVACION DIGITAL</b></p>	<p><b>Código: ANL04</b></p>
		<p><b>Versión: 2</b></p>

colaboración y el apoyo, mediante la consolidación en un ambiente de respeto y apertura en las relaciones interpersonales, que aporten al desarrollo de la ética y al compromiso ciudadano.

**Convivencia:** Al acoger la condición social del Hombre, la Institución establece como uno de sus principios básicos el de la convivencia de sus participantes, mediante el respeto mutuo y el tratamiento constructivo de la divergencia de ideas y el acatamiento a los principios de la dignidad humana.

**Transparencia:** Uno de los fundamentos de la acción Institucional es la transparencia, entendida como la rectitud y coherencia en el obrar y la disposición permanente de hacer públicos todos sus actos.

**Participación:** En su labor de formar ciudadanos, promueve actitudes críticas y fomenta la participación ciudadana, estimula el trabajo en equipo, la cooperación y ofrece respuestas a los retos que impone la democracia.

**Uso de las tecnologías de la comunicación (TIC):** Las nuevas tecnologías de la Información y Comunicación son aquellas herramientas computacionales e informáticas que procesan, almacenan, sintetizan, recuperan y presentan información representada de la más variada forma y constituyen nuevos soportes y canales para transmitir, compartir y socializar el conocimiento y por ello se convierten en medios e instrumentos importantes en la Institución o para mejorar la gestión administrativa y académica para dinamizar los procesos de enseñanza-aprendizaje y para llegar a nuevos públicos, ampliando el radio de acción social de la Institución.

**Internacionalización:** Mediante este proceso la Institución viabiliza la globalización de la enseñanza y el aprendizaje universitario. Es la forma como se estrechan los vínculos y niveles de integración con las diferentes instituciones de educación superior, en el ámbito internacional para dinamizar el intercambio científico, técnico, tecnológico y cultural de: directivos, profesores y estudiantes, así como el aprendizaje de los contenidos curriculares donde el conocimiento respectivo se reproduzca sin importar su ubicación espacial.

**Medio ambiente:** Tiene en cuenta en su actuar al entorno que afecta y condiciona especialmente las circunstancias de vida de las personas o la sociedad su conjunto en el entendido de que el medio ambiente comprende el conjunto de valores naturales, sociales y culturales existentes en un lugar y un

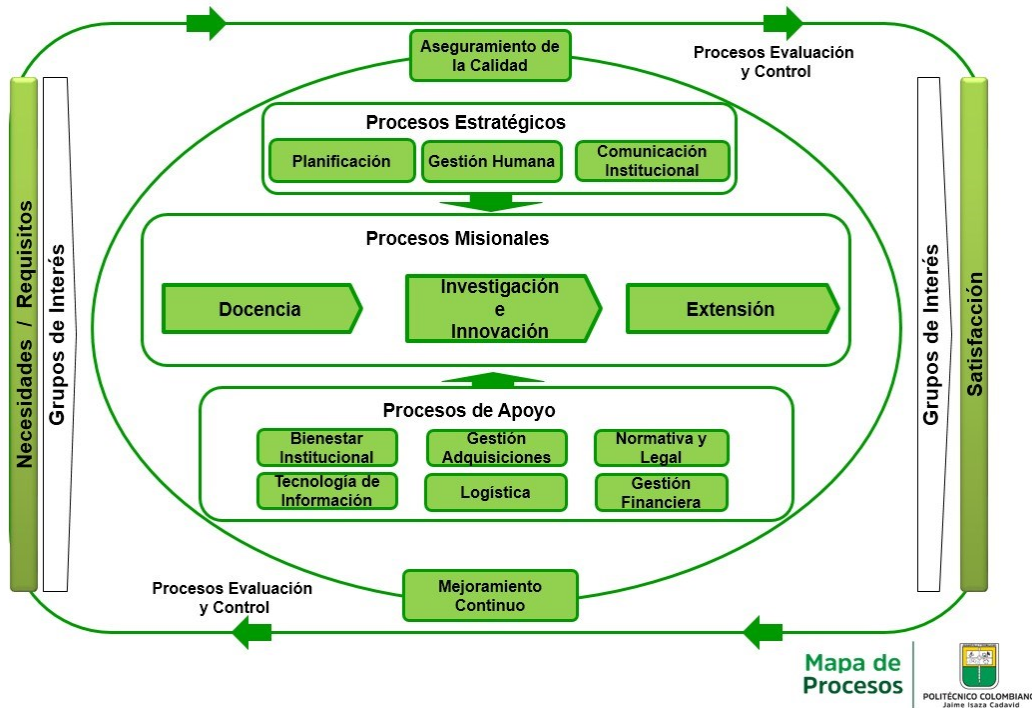
 POLITÉCNICO COLOMBIANO JAIME ISAZA CADAVID	<b>PLAN DE PRESERVACION DIGITAL</b>	<b>Código: ANL04</b>
		<b>Versión: 2</b>

momento determinado, que influyen en la vida del hombre y en las generaciones venideras. Es decir, no se trata sólo del espacio en el que se desarrolla la vida, sino que también abarca elementos tan intangibles como la cultura y por ello la institución debe contribuir a la formación de los estudiantes en la concepción científica del mundo y la comprensión de los problemas del medio ambiente, del desarrollo sostenible y de la necesidad de la educación ambiental y su vínculo con la sociedad.

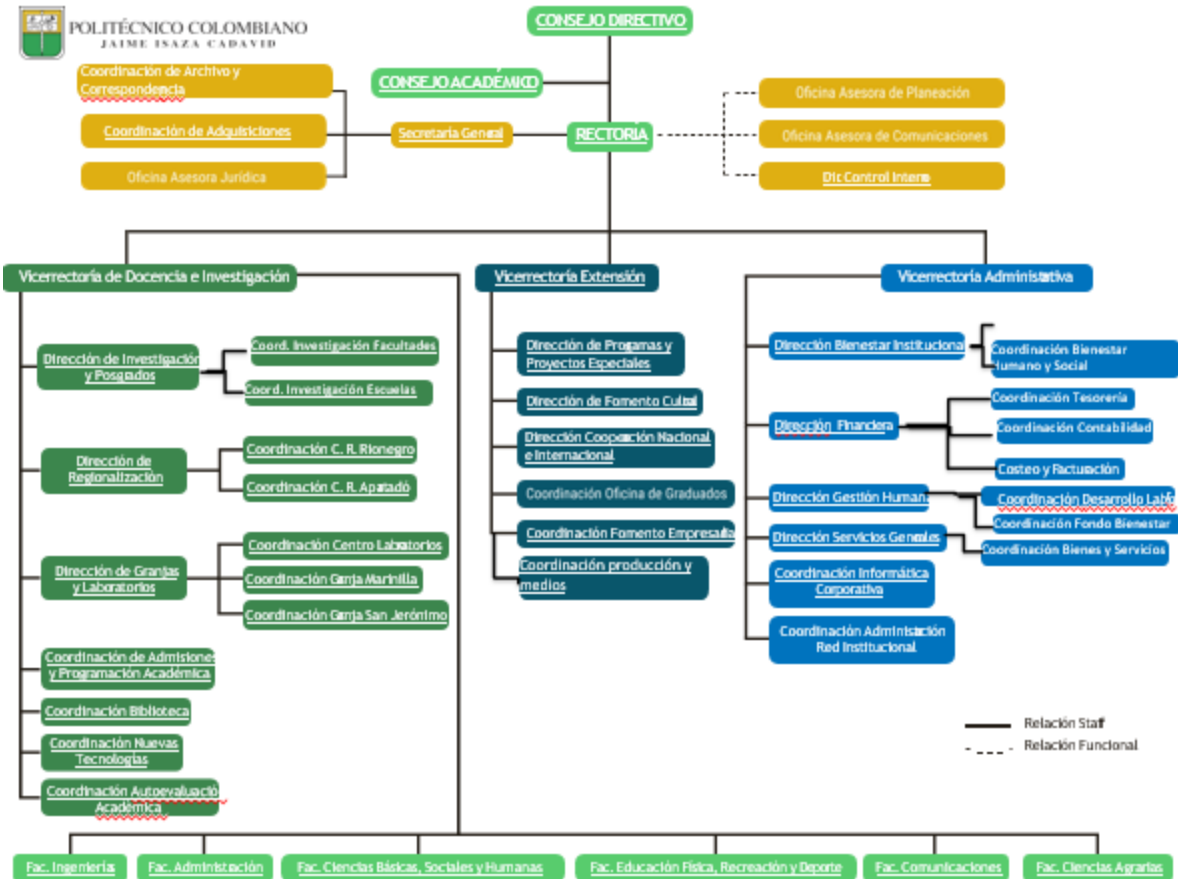
Bienestar: En cumplimiento de sus objetivos adopta como principio el mejoramiento de la calidad de vida y el desarrollo integral de todos los miembros de la Comunidad Politécnica, igualmente brinda bienestar y contribuye a la formación integral del ser.

### Mapa de Procesos

La Institución cuenta con una gestión por procesos y para ello construyó un mapa de procesos acorde con su misión y visión y que a continuación se presenta:



### Organigrama:



### 3.2. ANÁLISIS DE REFERENTES NORMATIVOS

Si bien es cierto hay una amplia gama de normas nacionales e internacionales sobre el tema de la preservación digital a largo plazo, a continuación, se presenta un compendio de las normas principales relacionadas con este importante tema y que pretenden dar una ilustración sobre los conceptos principales:

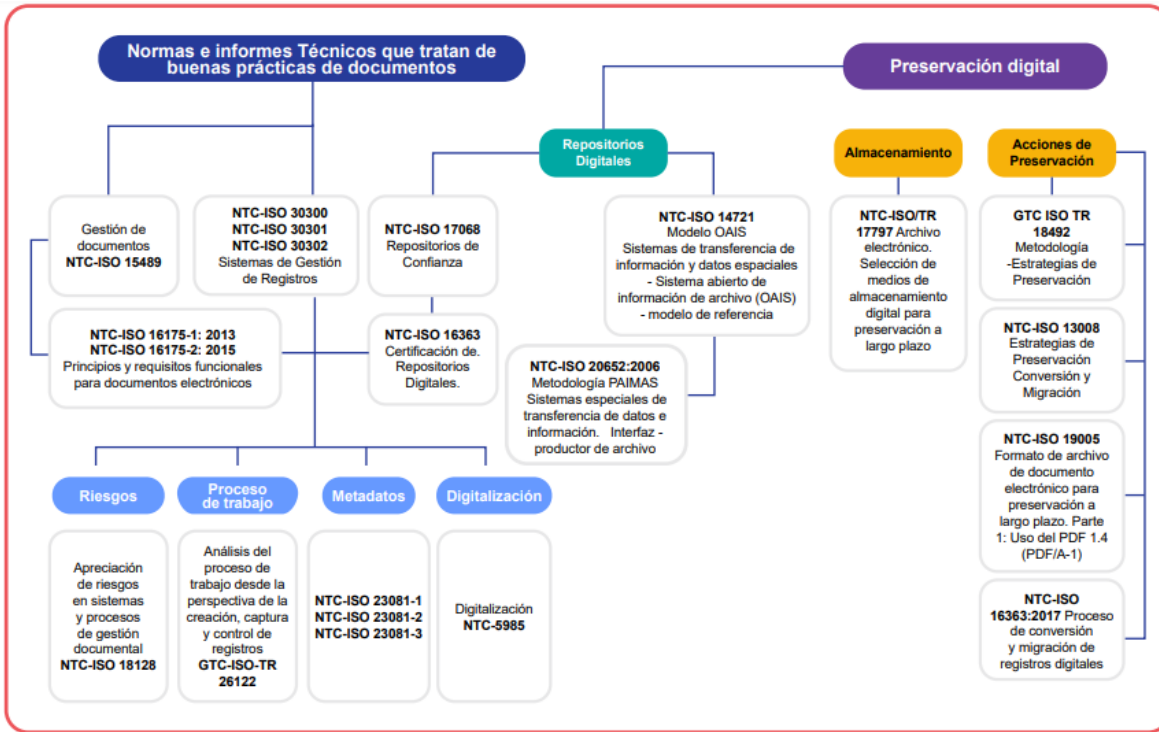


Imagen tomada de la Guía para la Elaboración e Implementación del Plan de Preservación Digital

#### 4. FASES PARA LA ELABORACIÓN DEL PLAN DE PRESERVACIÓN DIGITAL - PPD-

##### 4.1. Fase 1 Bases del PPD

##### 4.1.1. Objetivos

##### Objetivo General

Definir los procesos y estrategias para garantizar la preservación digital, el uso y acceso a los documentos electrónicos de archivo y otros objetos digitales del Politécnico Colombiano Jaime Isaza Cadavid, de tal manera que se asegure que todas las partes interesadas puedan acceder a estos.

##### Objetivos específicos

- Definir los procesos y procedimientos para garantizar la preservación digital a largo plazo de los documentos electrónicos y objetos digitales de la Institución.
- Documentar los procesos y procedimientos para mejorar la eficiencia, reducir

 <p>POLITÉCNICO COLOMBIANO JAIME ISAZA CADAVID</p>	<p><b>PLAN DE PRESERVACION DIGITAL</b></p>	<p><b>Código: ANL04</b></p> <hr/> <p><b>Versión: 2</b></p>
--	--	--

errores y aumentar la calidad en la preservación a largo plazo de los documentos y objetos digitales que se producen y reciben en la Institución.

- Capacitar y difundir los procesos y procedimientos definidos para la preservación a largo plazo de los documentos electrónicos de archivo y objetos digitales de la Institución.

#### **4.1.2. Alcance**

El Plan de Preservación Digital -PPD- va desde la producción o recepción del documento u objeto digital y su registro en los sistemas de información de la Institución de acuerdo con la Política de Gestión Documental y con los diferentes procesos y lineamientos del proceso, con el apoyo de la Oficina de Informática Corporativa, pasando por su gestión, almacenamiento, seguridad de la información y preservación de estos, y debe ser acatado por todos los funcionarios y contratistas de las unidades académicas y administrativas de la Institución.

#### **4.1.3. Articulación con los programas institucionales**

En el Politécnico Colombiano Jaime Isaza Cadavid se sigue, en el proceso de Gestión Documental, la aplicación de la política de eficiencia administrativa del estado colombiano, establecido en el modelo Integrado de Planeación y Gestión (MIPG), el cual determina la gestión de calidad, eficiencia el uso de recursos (Cero Papel), racionalización de trámites, modernización institucional y gestión de tecnologías de información.


Para integrar las funciones, acciones y responsabilidades, mejoramiento continuo y satisfacción de las partes interesadas, la Institución determinará en el plan estratégico institucional y los planes de acción anual las actividades que garanticen la efectividad de la armonización del PGD con los diferentes sistemas del Sistema de Gestión Integrado de la Entidad.

Por otra parte, teniendo en cuenta las acciones que se enmarcan en el Plan de Preservación Digital, es importante que este se encuentre alineado con las diferentes políticas, planes, programas y procesos de la Institución, con el fin de asegurar que las actividades, estrategias y metodologías planteadas se implementen de manera eficiente y eficaz.

Para identificar claramente la interacción con las diferentes políticas, planes y programas institucionales, se presenta la siguiente matriz, indicando los objetivos de cada uno de los descritos en esta e indicando la forma como se articulan, integran, complementan, acoplan o reflejan dentro de otros documentos:

	<b>PLAN DE PRESERVACION DIGITAL</b>	<b>Código: ANL04</b>
		<b>Versión: 2</b>

POLITICA, PLAN O PROGRAMA	OBJETIVO	ARTICULACIÓN
<b>Sistema Integrado de Gestión</b>	Mejorar la gestión institucional mediante el aprovechamiento de los recursos, las oportunidades que ofrece el entorno y la autorregulación de sus procesos.	El Plan de Preservación Digital presenta indicadores de evaluación y control en cuanto al crecimiento en el almacenamiento digital y los riesgos de la preservación digital.
<b>Sistema de Gestión Ambiental</b>	Fomentar los componentes de gestión ambiental buscando prevenir, mitigar, minimizar y/o controlar los impactos ambientales negativos derivados de las actividades académicas y administrativas que puedan afectar el entorno del Politécnico Colombiano Jaime Isaza Cadavid.	El Plan de Preservación Digital aporta a la estrategia de cero papel acorde con la Directiva Presidencias 04 de 2012 sobre la disminución del uso de papel.
<b>Seguridad en la Información</b>	Establecer las políticas de seguridad y privacidad de la información del Politécnico Colombiano Jaime Isaza Cadavid, con el fin de mantener la disponibilidad, confidencialidad e integridad de la información por medio de planeación, ejecución y seguimiento de políticas que propendan por la seguridad informática institucional.	El Plan de Preservación Digital contempla la información digital que se encuentra en repositorios y, por ende, se debe garantizar la disponibilidad, confidencialidad e integridad de la información por medio de planeación, ejecución y seguimiento de las políticas que propenden por la seguridad informática institucional.
<b>Plan Estratégico de Tecnologías de Información -PETI-</b>	El Plan Estratégico de Tecnologías de la Información (PETI) representa el norte a seguir por la entidad durante el periodo (2023 – 2025) y recoge las preocupaciones y oportunidades de mejoramiento de los interesados en lo relacionado con la gestión de TI para apoyar la estrategia y el modelo operativo de la organización apoyados en las definiciones de la Política de Gobierno Digital.	El Plan de Preservación Digital se articula con el PETI en los dominios definidos en el modelo de gestión Estrategia, Gobierno, Información, Sistemas de Información, Infraestructura de TI, Uso y Apropriación y Seguridad
<b>Plan de tratamiento de riesgos de seguridad y privacidad de la información</b>	Establecer el plan de tratamiento de riesgos informáticos del Politécnico Colombiano Jaime Isaza	El Plan de Preservación Digital se articula con este plan en cuanto que la Institución entiende la importancia de una

 POLITÉCNICO COLOMBIANO JAIME ISAZA CADAVID	<b>PLAN DE PRESERVACION DIGITAL</b>		<b>Código: ANL04</b>
			<b>Versión: 2</b>
	<p>Cadavid, con el fin de mantener la disponibilidad, confidencialidad e integridad de la información de acuerdo con la criticidad establecida en los activos de información.</p>	<p>adecuada gestión de la información, y se ha comprometido con la implementación de un plan de tratamiento de los riesgos informáticos que busca establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, y garantizar la seguridad y privacidad de su información.</p>	
<b>Modelo Integrado de Planeación y Gestión</b>	<p>El Modelo Integrado de Planeación y Gestión -MIPG- es el sistema integrado por el esquema de organización y el conjunto de los planes, métodos, principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por El Politécnico Colombiano Jaime Isaza Cadavid,</p>	<p>El Plan de Preservación Digital se articula con MIPG en la dimensión 5 Información y comunicación, que tiene como propósito utilizar la información de manera adecuada y comunicarla por los medios y en los tiempos oportunos.</p>	

#### 4.1.4. Roles y responsabilidades

El plan de preservación digital es una estrategia que define las acciones necesarias para garantizar la longevidad y accesibilidad de la información digital a largo plazo. La implementación exitosa de este plan depende en gran medida de la asignación clara de los roles y responsabilidades. Al involucrar a los equipos adecuados y establecer procesos claros, la Institución puede garantizar la preservación a largo plazo de sus valiosos activos de información digitales, lo cual requiere una colaboración estrecha entre diferentes equipos y áreas de la organización.

A continuación, se detallan los roles clave y sus respectivas funciones y responsabilidades:

Roles Clave	Funciones	Responsabilidades
<b>Comité Institucional de Gestión y Desempeño</b>	<ul style="list-style-type: none"> <li>Aprobar la política de preservación digital.</li> <li>Asigna recursos y supervisa la implementación del plan.</li> </ul>	<ul style="list-style-type: none"> <li>Toma decisiones estratégicas sobre la preservación de los activos digitales</li> </ul>
<b>Oficina de Informática Corporativa</b>	<ul style="list-style-type: none"> <li>Coordina las actividades diarias de preservación.</li> </ul>	<ul style="list-style-type: none"> <li>Implementación de la infraestructura:</li> </ul>




POLITÉCNICO COLOMBIANO  
JAIME ESCALA CADAVID

## PLAN DE PRESERVACION DIGITAL

Código: ANL04

Versión: 2

- |   |   |   |
|---|---|---|
|   | <ul style="list-style-type: none"> <li>• Supervisa la migración de datos y la gestión de formatos.</li> <li>• Monitorea la integridad de los datos y la infraestructura</li> <li>• Implementa medidas de seguridad para proteger los datos de acceso no autorizado, pérdida y corrupción.</li> <li>• Gestiona la infraestructura tecnológica necesaria para la preservación digital.</li> <li>• Selecciona y configura el hardware y software adecuados.</li> </ul> | <p>Configurar y mantener la infraestructura tecnológica necesaria para la preservación digital.</p> <ul style="list-style-type: none"> <li>• Migración de datos: Transferir los datos a formatos y sistemas de almacenamiento adecuados para garantizar su longevidad.</li> <li>• Monitoreo y mantenimiento: Monitorear continuamente la integridad de los datos y la infraestructura, y realizar las acciones correctivas necesarias.</li> <li>• Colaboración con otras áreas: Colaborar con otras áreas de la organización para garantizar la integración de la preservación digital en los procesos de negocio.</li> </ul> |
| <p><b>Coordinación de Archivo y Correspondencia</b></p> | <ul style="list-style-type: none"> <li>• Crea y gestiona metadatos descriptivos para los activos digitales.</li> <li>• Garantiza que los metadatos sean</li> </ul>  | <ul style="list-style-type: none"> <li>• Identificar qué activos digitales requieren preservación y evaluar su valor a largo plazo.</li> </ul>  |

 <p>POLITÉCNICO COLOMBIANO JAIME ESCALA CADAVID</p>	<p><b>PLAN DE PRESERVACION DIGITAL</b></p>	<p><b>Código: ANL04</b></p> <hr/> <p><b>Versión: 2</b></p>
	<p>completos, precisos y conformes a los estándares.</p> <ul style="list-style-type: none"> <li>• Identifica y mitiga los riesgos asociados a la obsolescencia de los formatos.</li> </ul>	<ul style="list-style-type: none"> <li>• Crear políticas y procedimientos para la gestión de la preservación digital, incluyendo la selección de formatos, la migración de datos y la gestión de riesgos.</li> <li>• Capacitación: Proporcionar capacitación al personal sobre las políticas y procedimientos de preservación digital.</li> </ul>

### Consideraciones Adicionales

Adaptación a las tecnologías emergentes: Es importante estar al tanto de las últimas tecnologías y tendencias en el campo de la preservación digital para garantizar la sostenibilidad del plan a largo plazo.

Evaluación continua: El plan de preservación digital debe ser evaluado y actualizado regularmente para reflejar los cambios en los requisitos y las tecnologías.

## 4.2. Fase 2 Diagnóstico

### 4.2.1. Identificación de documentos electrónicos a preservar

En la actualidad, el Politécnico cuenta con un Software de gestión de documentos (SGDEA) denominado “*Mercurio*” donde se publican formatos y formularios electrónicos, los cuales llegan a convertirse en documentos electrónicos de archivo y que incorporan una firma mecánica electrónica asociada a cada usuario. Así mismo, la Institución cuenta con un Sistema de Gestión Integral en el software conocido como “*Mejoramiso*” que controla la producción y creación de formatos a través del procedimiento “PPL01 Procedimiento para la elaboración y control de documentos y registros”, el cual establece las directrices en la creación y actualización de los documentos contemplados en este y se cuenta con un listado maestro de documentos donde se tienen definidos 660 formatos que se usan en los 14 procesos y 4 subprocesos definidos en el mapa de procesos institucional, la Gestión Documental

 <p>POLITÉCNICO COLOMBIANO JAIME ESCALA CADAVID</p>	<p><b>PLAN DE PRESERVACION DIGITAL</b></p>	<p><b>Código: ANL04</b></p> <hr/> <p><b>Versión: 2</b></p>
---	--	--

de la Institución se encuentra soportada y documentada a través de 27 documentos entre Procedimientos, Guías, Formatos, Planes e Instructivos acorde a la normatividad vigente.

Por otro lado, la Institución cuenta con el Software UNIVERSITAS XXI (Sistema de Información y Control Académico) donde se ejecutan actividades académicas y administrativas a través de medio electrónico, POLIDINAMICO (Intranet), BIBLIOTECA Y PRIMO (Bases de datos bibliográficas), POLIVIRTUAL (e-learning), MESA DE AYUDA (Soporte técnico informático) en los cuales se genera información electrónica para la gestión y trámite de estudiantes, empleados, contratistas y docentes, se indican algunos criterios para el manejo de los correos electrónicos, se realizan las inscripciones y matrículas de estudiantes, entre otras actividades que inciden en la creación de documentos electrónicos a los cuales se debe garantizar su preservación a largo plazo.

El Programa de Normalización de Formas y Formularios Electrónicos y el Programa de Documentos Electrónicos de Archivo son herramientas archivísticas con que cuenta la Institución y que se enfocan en los procesos de planeación, producción y control documental, puesto que buscan identificar las características para los documentos electrónicos producidos por la Institución, el cumplimiento sostenido en la producción de los documentos de dichas características conlleva naturalmente al establecimiento de la tradición documental, entendida esta como la costumbre de transmitir o generar el documento<sup>3</sup>.

### **Inventario dispositivos o medios de almacenamiento**

A través de la “Tabla 1 Inventario de dispositivos o medios de almacenamiento”, se identificaron los medios de almacenamiento, ubicación y accesibilidad a ellos, donde se encuentran los documentos electrónicos a preservar en la Institución (Ver Tabla 1).

También se realizó un inventario de documentos digitalizado que serán preservados a largo plazo y que se puede ver en la “Tabla 2 Inventario de documentos digitalizados” (Ver Tabla 2)

<sup>3</sup> Definición referenciada en: Heredia Herrera, Antonia. Forma y formato de los documentos de archivo. Boletín ANABAD. LXVII (2017), NÚM. 4, OCTUBRE-DICIEMBRE. MADRID. ISSN: 2444-0523 (CD-ROM). Consultado en: <https://dialnet.unirioja.es/servlet/articulo?codigo=6449987>

 POLITÉCNICO COLOMBIANO JAIME ESCALA CADAVID	<b>PLAN DE PRESERVACION DIGITAL</b>	<b>Código: ANL04</b>
		<b>Versión: 2</b>

**Tabla 1 Inventario Dispositivos o Medios de Almacenamiento**

TIPO DE ALMACENAMIENTO	CANTIDAD	CAPACIDAD	UBICACIÓN FISICA	ACCESIBILIDAD	AÑO DE ADQUISICIÓN	No de Documentos electrónicos	Tamaño total de los documentos
<i>CDs, DVDs, Blu-Ray</i>							
<i>Discos Duros</i>							
<i>Medios magnéticos: Discos rígidos, cintas magnéticas, diskettes, etc.</i>							
<i>Medios electrónicos: Discos SSD, pendrives, tarjetas de memoria, etc.</i>							
<i>Servidores</i>							
<i>Nube</i>							


 POLITÉCNICO COLOMBIANO JAIME ESCALA CADAVID	<b>PLAN DE PRESERVACION DIGITAL</b>	<b>Código: ANL04</b>
		<b>Versión: 2</b>

**Tabla 2 Cantidad documentos digitales**

Fondo	Sección	Cantidad de Imágenes	Tamaño	Ubicación	Observaciones

**Matriz de identificación en el repositorio de preservación digital**

Detalle	Cantidad	Formatos	Distribución
Archivos en formatos de compatibles para preservación	762897 73,3%	Pdf (sin certeza de cumplimiento con PDF/A) Tiff y XML.	- 43,4% Radicados -35,9% Anexo expediente - 20,7% Anexo a radicado
Archivos en formatos identificados netamente para distribución	278604 26,8%	doc; docx, html, jpg, html, xls, xlsx, xlsx, png, zip, jpeg	- 76,5% Anexo a radicado - 23,3% Radicados - 0,2% Anexos expedientes
Archivos en otros formatos	5070 0,5%	Principalmente msg; rtf; rar, entre otros	-92,3% Anexo a radicado -3,9% Anexo a expediente -3,7% Radicado
Total de archivos identificados			1040691

	<b>PLAN DE PRESERVACION DIGITAL</b>	<b>Código: ANL04</b>
		<b>Versión: 2</b>

#### 4.2.2. Diagnóstico de los documentos electrónicos a preservar

En un mundo cada vez más digital, la gestión eficiente de los documentos se ha convertido en una necesidad imperiosa. La gestión de documentos electrónicos de archivo es necesaria en la Institución para organizar, preservar y recuperar los archivos digitales de manera segura y confiable, por ello, es imperativo identificar los documentos electrónicos de archivo institucionales para definir y presentar las posibilidades con las que cuenta el POLI para acceder a sus documentos desde cualquier lugar y en cualquier momento, simplificando los procesos y mejorando la colaboración entre los funcionarios. Además, ante esta era digital, es necesario definir los estándares de seguridad y confidencialidad, para garantizar la protección de la información Institucional.

El proceso de gestión documental tiene definidos ocho (8) procesos según el Decreto 1080 de 2015, los cuales se sustentan en una serie de instrumentos archivísticos que lo fortalecen y lo hacen funcional, así como otras actividades administrativas y técnicas para la planificación, gestión y organización de la documentación producida y recibida por las Entidades, desde su origen hasta su disposición final para lograr una administración efectiva de la información. Los procesos mencionados son los siguientes:



Fuente: Elaboración propia. Procesos de la gestión documental indicados en el Decreto 1080 de 2015, art. 3.8.3.5.9

Imagen tomada de [https://www.metrodebogota.gov.co/sites/default/files/instrumentos\\_gestion\\_informacion/GD-DR-001-Programa-de-Gestion-Docamental\\_V.03.pdf](https://www.metrodebogota.gov.co/sites/default/files/instrumentos_gestion_informacion/GD-DR-001-Programa-de-Gestion-Docamental_V.03.pdf)

 <p>POLITÉCNICO COLOMBIANO JAIME ISAZA CADAVID</p>	<p><b>PLAN DE PRESERVACION DIGITAL</b></p>	<p><b>Código: ANL04</b></p> <hr/> <p><b>Versión: 2</b></p>
--	--	--

Actualmente, el Politécnico Colombiano Jaime Isaza Cadavid está enfocado en seguir un camino hacia una gestión de documentos electrónicos, siguiendo lo definido por el gobierno nacional y de acuerdo con el Decreto 1080 de 2015, en los cuales, uno de los objetivos principales es el de simplificar y racionalizar los tramites a través de medios electrónicos, facilitando a los ciudadanos el acceso a la información pública.

Es por ello por lo que se realiza la identificación de aquellos documentos electrónicos de archivo generados por los funcionarios en cumplimiento de sus funciones para poder definir las estrategias para la gestión y control de ellos para minimizar los riesgos de pérdida de información y asegurar su preservación a largo plazo.

Para poder realizar la identificación de los documentos electrónicos a preservar, se recurrió a las funciones definidas dentro del Manual de Funciones y Competencias Laborales, de conformidad con la Resolución Rectoral No. 201905000296 de mayo 8 de 2019, Acuerdo No.11 del 10 de junio de 2019, Resolución Rectoral No. 201905000853 de octubre 28 de 2019, Resolución Rectoral No. 202005000269 del 26 de junio de 2020, Resolución No. 202105000084 de febrero 22 de 2021 y Resolución Rectoral No. 2023050000156 del 16 de marzo de 2023 y demás normas concordantes, tomando como punto de partida la actual estructura orgánico funcional.

Posteriormente, se realizó un análisis y verificación de los procesos, procedimientos y funciones establecidos para cada una de las oficinas productoras, se identificó la producción documental con el propósito de asociar las series y subseries documentales existentes, logrando la consolidación de estas y sus tipos documentales, las cuales se encuentran soportadas en los actos administrativos de la institución (acuerdos, resoluciones, circulares, manuales, etc.).

Por otra parte, se realizaron entrevistas a los funcionarios productores y custodios de la información y se recopilaron los antecedentes frente a la producción documental y la dinámica de la gestión y trámite adelantado al interior de la(s) dependencia(s) y su operación e interrelación con otras oficinas.

Como resultado del análisis e interpretación de la información y la producción documental identificada, se consolidó la información recopilada, se analizó y se conformaron las series y subseries documentales con sus respectivos tipos documentales, identificando su procedencia, así como el soporte en el cual eran generados (Papel, Electrónico o ambos) dentro de su ciclo vital.

Fue así como se elaboraron las Tablas de Retención Documental para la aplicación de los principios y procesos archivísticos, a fin de garantizar la protección del patrimonio documental; atendiendo entre otros aspectos a la valía de la información que se produce en cumplimiento de los fines misionales de la institución y aquellos que hacen parte de la gestión diaria de la misma y donde se pudo identificar los documentos electrónicos de archivo que

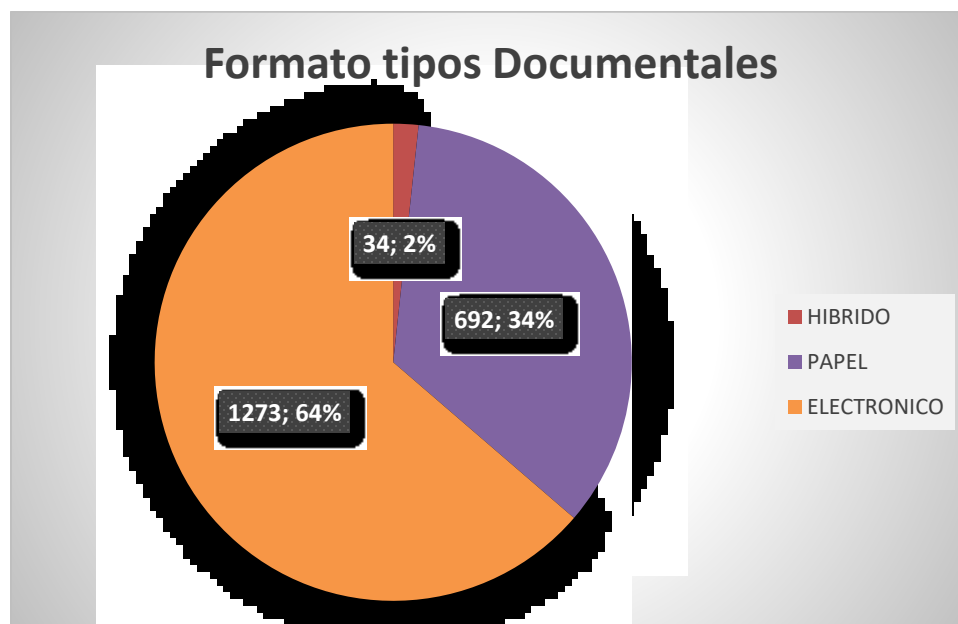
	<b>PLAN DE PRESERVACION DIGITAL</b>	<b>Código: ANL04</b>
		<b>Versión: 2</b>

se generan en la institución por los funcionarios en cumplimiento de sus funciones y que se publican en el Software de Gestión Electrónica de Documentos “Mercurio”, el resultado de ese ejercicio se presenta en el siguiente cuadro:

**Tabla 3 Cantidad Tipos Documentales por formato**

<b>TOTAL TIPOS DOCUMENTALES IDENTIFICADOS</b>	<b>560</b>	
<b>HIBRIDO</b>	<b>34</b>	<b>2%</b>
<b>PAPEL</b>	<b>692</b>	<b>34%</b>
<b>ELECTRONICO</b>	<b>1273</b>	<b>64%</b>

**Gráfico 1 Porcentaje tipos documentales por formato**



#### **4.2.3. Análisis de riesgos**

Uno de los principales objetivos de la preservación digital es identificar y valorar los riesgos en el tema tecnológico para definir las estrategias para minimizarlos para una efectiva gestión de estos, de tal forma que se garantice la seguridad e integridad de los objetos digitales o electrónicos.

En ese sentido, la Institución tiene identificados sus riesgos en el proceso de Tecnologías de la Información cuyo objetivo es *“Proporcionar soluciones y servicios efectivos de TI a la comunidad institucional, haciendo uso eficiente de la gestión del conocimiento y las nuevas tecnologías para promover acciones innovadoras que apoyen los procesos institucionales, permitiendo a nuestros usuarios optimización y competitividad, contribuyendo de esta*

 POLITÉCNICO COLOMBIANO JAIME ESCALA CADAVID	<b>PLAN DE PRESERVACION DIGITAL</b>	<b>Código: ANL04</b>
		<b>Versión: 2</b>


*manera al desarrollo económico, social y ambiental del Politécnico”, y el alcance va desde la gestión administrativa, de alineamiento, organización y planeación de TI hasta la administración de la seguridad y privacidad de la información.*

En la siguiente tabla se identifican y valoran los riesgos asociados a las tecnologías de la información y que afectan la preservación digital a largo plazo en la Institución<sup>4</sup>:

---


<sup>4</sup> Para ampliar la información y el detalle de los riesgos identificados, consultar el mapa de riesgos institucional

 POLITÉCNICO COLOMBIANO JAIME ESCALA CADAVID	<b>PLAN DE PRESERVACION DIGITAL</b>	<b>Código: ANL04</b>
		<b>Versión: 2</b>

 POLITÉCNICO COLOMBIANO JAIME ESCALA CADAVID			
<b>IDENTIFICACIÓN DE RIESGOS ASOCIADOS A LAS TIC</b>			
<b>CLASIFICACION DEL RIESGO SEGÚN EL ACTIVO</b>	<b>RIESGOS</b>	<b>CAUSA</b>	<b>CONSECUENCIAS</b>
<b>PERDIDA DE CONFIDENCIALIDAD</b>	Abuso de derechos	<ul style="list-style-type: none"> <li>• Privilegios de acceso excesivo o inutilizado</li> <li>• Uso abusivo de los privilegios asignados</li> </ul>	Abuso de los derechos por Privilegios otorgados permitiendo excesos en el acceso a los activos informáticos, lo que podría causar la pérdida de confidencialidad sobre los activos de información
<b>PERDIDA DE CONFIDENCIALIDAD</b>	Hurto de medios o documentos	<ul style="list-style-type: none"> <li>• Falta de protección de las copias de seguridad</li> <li>• Falta de cuidado en gestión de la información sensible</li> <li>• Ausencia de un eficiente control de cambios en la configuración</li> </ul>	Falta de protección de las copias de seguridad y de cuidado en gestión de la información sensible pueden permitir su hurto, lo que podría causar la pérdida de confidencialidad de la información. La falta de políticas de seguridad, de control de acceso físico, mecanismos de autenticación débil, pueden facilitar el hurto, lo cual causaría la pérdida de la confidencialidad en el hardware

 POLITÉCNICO COLOMBIANO JAIME ESCALA CADAVID	<b>PLAN DE PRESERVACION DIGITAL</b>	<b>Código: ANL04</b>
		<b>Versión: 2</b>

<b>PERDIDA DE CONFIDENCIALIDAD</b>	<ul style="list-style-type: none"> <li>• Abuso de los derechos</li> <li>• Error en el uso</li> <li>• Falsificación de derechos</li> <li>• Procesamiento ilegal de datos</li> <li>• Mal funcionamiento del software</li> </ul>	<ul style="list-style-type: none"> <li>• Ausencia de “terminación de sesión” cuando se abandona la estación de trabajo</li> <li>• Asignación errada de los derechos de acceso.</li> <li>• Configuración incorrecta de parámetros</li> <li>• Ausencia de mecanismos de identificación y autenticación</li> <li>• Habilidad de servicios innecesarios</li> <li>• Software nuevo o inmaduro</li> <li>• Almacenamiento sin protección física</li> <li>• Falta de cuidado en la disposición final Copia no controlada.</li> <li>• Ausencia de procedimientos para el manejo de información clasificada.</li> <li>• Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos</li> <li>• Ausencia de procedimiento formal para el registro y retiro de usuarios</li> </ul>	<p>Ausencia de mecanismos de identificación y autenticación puede ocasionar abuso de derechos error en el uso lo que causaría pérdida de confidencialidad en el software o posibilidad de acceso a S.O, manejadores de Bases de Datos y/o software institucional, sin ningún tipo de restricción.</p> <p>Almacenamiento sin protección física y falta de cuidado en la disposición final o Copia no controlada que facilita el error en el uso posibilitando la pérdida de confidencialidad en el hardware.</p> <p>La ausencia de responsabilidades en seguridad de la información en las funciones del cargo, así como de procedimientos para el manejo de información clasificada y de registro y retiro de usuarios puede generar error en el uso y/o abuso de derechos, lo cual causaría pérdida de confidencialidad en el servicio</p>
<b>PERDIDA DE CONFIDENCIALIDAD</b>	Procesamiento ilegal de los datos	<ul style="list-style-type: none"> <li>• Ausencia de mecanismos de monitoreo</li> </ul>	<p>La ausencia de mecanismos de monitoreo puede facilitar el procesamiento ilegal de los datos, lo cual podría generar pérdida de confidencialidad de los procesos realizados por el personal</p>

 POLITÉCNICO COLOMBIANO JAIME ESCALA CADAVID	<b>PLAN DE PRESERVACION DIGITAL</b>	<b>Código: ANL04</b>
		<b>Versión: 2</b>

<b>PERDIDA DE CONFIDENCIALIDAD</b>	Reprocesos en la gestión de los Sistemas de información institucional	<ul style="list-style-type: none"> <li>• Ausencia de políticas de control de acceso a bases del conocimiento con información reservada</li> </ul>	La ausencia de políticas de control de acceso a bases del conocimiento con información reservada pueden facilitar el reproceso en la gestión de los sistemas de información lo que causaría pérdida de confidencialidad de los intangibles.
<b>PERDIDA DE INTEGRIDAD</b>	Abuso de los derechos	<ul style="list-style-type: none"> <li>• Privilegios de acceso excesivo o inutilizado</li> <li>• Uso abusivo de los privilegios asignados</li> </ul>	Los privilegios de acceso excesivo o inutilizado pueden facilitar el abuso de los derechos lo que causaría la pérdida de integridad de la información.
<b>PERDIDA DE INTEGRIDAD</b>	<b>Corrupción de datos</b>	<ul style="list-style-type: none"> <li>• Errores en aplicativos web que permiten la infiltración de código malicioso.</li> <li>• Falta o desactualización del software de ciberseguridad</li> <li>• Falta de diagnóstico de vulnerabilidades</li> </ul>	Errores en aplicativos web que producen vulnerabilidades y la falta de actualización del software de seguridad así como la ausencia de diagnóstico de vulnerabilidades provocaría corrupción de datos, cual causaría pérdida de integridad de la información

	<b>PLAN DE PRESERVACION DIGITAL</b>	<b>Código: ANL04</b>
		<b>Versión: 2</b>

#### 4.2.4. Evaluación de la capacidad de preservación digital en la entidad

El Politécnico Colombiano Jaime Isaza realizó un diagnóstico para evaluar su capacidad de preservación digital, basado en el modelo de madurez para medir este aspecto, que se encuentra en la Guía Para la Elaboración e Implementación del Plan de Preservación Digital del Archivo General de la Nación<sup>5</sup>.

Este modelo está basado en el Modelo de Madurez Para Medir la Capacidad de Preservación Digital (DPCMM por sus siglas en inglés) del Council Of State Archivists (CoSA) el cual es un marco que se basa en funciones del Open Information Archival System (OAIS) que es un modelo internacional de referencia que define los procesos necesarios para preservar y acceder a los objetos de información de forma efectiva y a largo plazo, y establece un lenguaje común que los describe, y que fue acogido por la Norma ISO 14721, que recoge criterios de auditoría de repositorios confiables (ISO 16363), y que se utiliza para evaluar las capacidades de preservación digital de una Entidad en un momento determinado.

El modelo se basa en 15 componentes que definen diferentes capacidades en la gestión de preservación digital, las cuales son: Política, Estrategia, Gobernanza, Colaboración, Experiencia Técnica, Formatos de Fuente Abierta/Neutral, comunidad Designada, Encuesta de Registros Electrónicos, Ingesta, Almacenamiento, Renovación de Dispositivos/Medios, Integridad, Seguridad, Metadatos y Acceso, los cuales se delimitan y sitúan en cinco (5) diferentes etapas evolutivas de trabajo en preservación digital de la Institución y se evalúan con puntajes que van desde la etapa a 1 (Nominal) hasta la etapa 5 (óptima) con números de 0 a 4 (Ver imagen)

**Ilustración 4.2.4-1 Etapas y puntuación evaluación preservación digital**

<b>Nominal</b>	<b>Mínimo</b>	<b>Intermedio</b>	<b>Avanzado</b>	<b>Óptimo</b>
<b>0</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>

Las cinco (5) etapas evaluadas obtienen un puntaje que indica los niveles de capacidad de madurez en cuanto a la preservación digital con el cual cuenta la Institución, como se aprecia en la imagen:

<sup>5</sup> Esta Guía se encuentra publicada en [https://www.archivogeneral.gov.co/sites/default/files/Estructura\\_Web/5\\_Consulte/Recursos/Publicaciones/2022/GuiaPlanPreservacionDigital.pdf](https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/5_Consulte/Recursos/Publicaciones/2022/GuiaPlanPreservacionDigital.pdf)

	<b>PLAN DE PRESERVACION DIGITAL</b>	Código: ANL04
		Versión: 2

**Ilustración 4.2.4-2 Niveles de capacidad de madurez en preservación digital**

Niveles de capacidad		Índice de puntuación
	<i>Capacidad de preservación digital nominal</i>	0
	<i>Capacidad mínima de conservación digital</i>	1 - 15
	<i>Capacidad de preservación digital intermedia</i>	16 - 30
	<i>Capacidad avanzada de conservación digital</i>	31 - 45
	<i>Capacidad de conservación digital óptima</i>	46 - 60

Luego de realizado el ejercicio y aplicado el modelo de evaluación de capacidad de Madurez en Preservación Digital para el Politécnico Colombiano Jaime Isaza Cadavid, el resultado fue el siguiente:

RESUMEN CUMPLIMIENTO	PUNTOS OBTENIDOS	RANGO DE PUNTO
<b>Capacidad de Preservación Digital Nominal</b>	0	0
<b>Capacidad Mínima de Conservación Digital</b>	3	1-15
<b>Capacidad de Preservación Digital Intermedia</b>	18	16-30
<b>Capacidad Avanzada de Conservación Digital</b>	3	31-45
<b>Capacidad de Conservación Digital Óptima</b>	0	46-60
<b>Total</b>	<b>24</b>	<b>60</b>

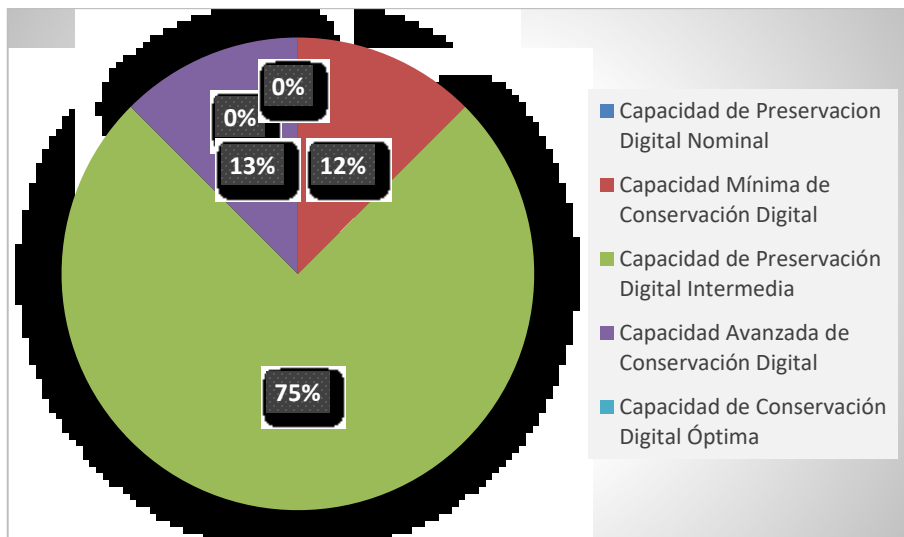
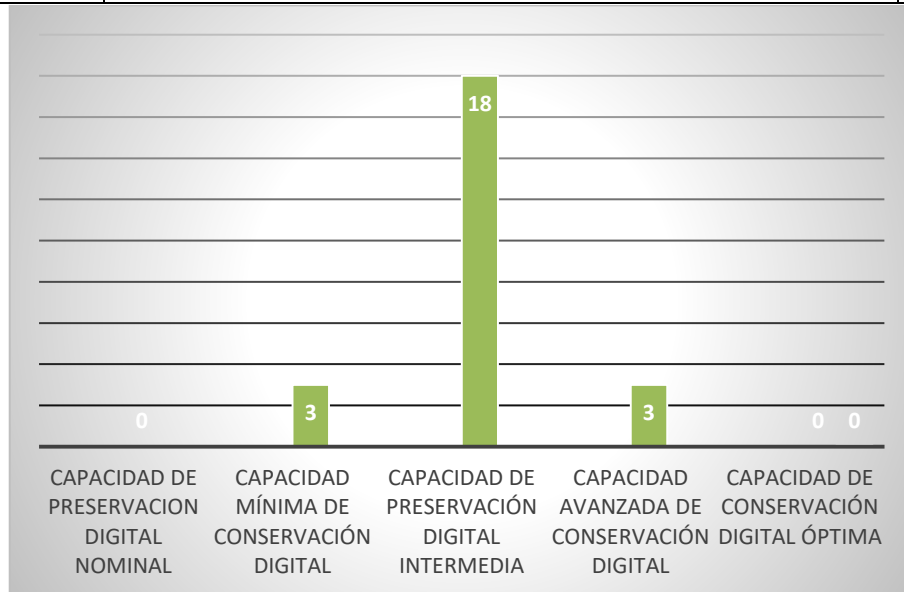


POLITÉCNICO COLOMBIANO  
JAIME ESCALA CADAVID

## PLAN DE PRESERVACION DIGITAL

Código: ANL04

Versión: 2



INDICE DE Puntuación		
0	NOMINAL	
1 - 15	MINIMA	
16 - 30	INTERMEDIA	X
31 - 45	AVANZADA	
46 - 60	OPTIMA	

Según el resultado del ejercicio, la capacidad de Preservación Digital en la Institución está en un nivel intermedio, con un puntaje de 24 sobre 60 para un cumplimiento de un 25%, por lo que se requiere de un plan estratégico para poder llevar las capacidades institucionales a

	<b>PLAN DE PRESERVACION DIGITAL</b>	<b>Código: ANL04</b>
		<b>Versión: 2</b>

niveles avanzados.

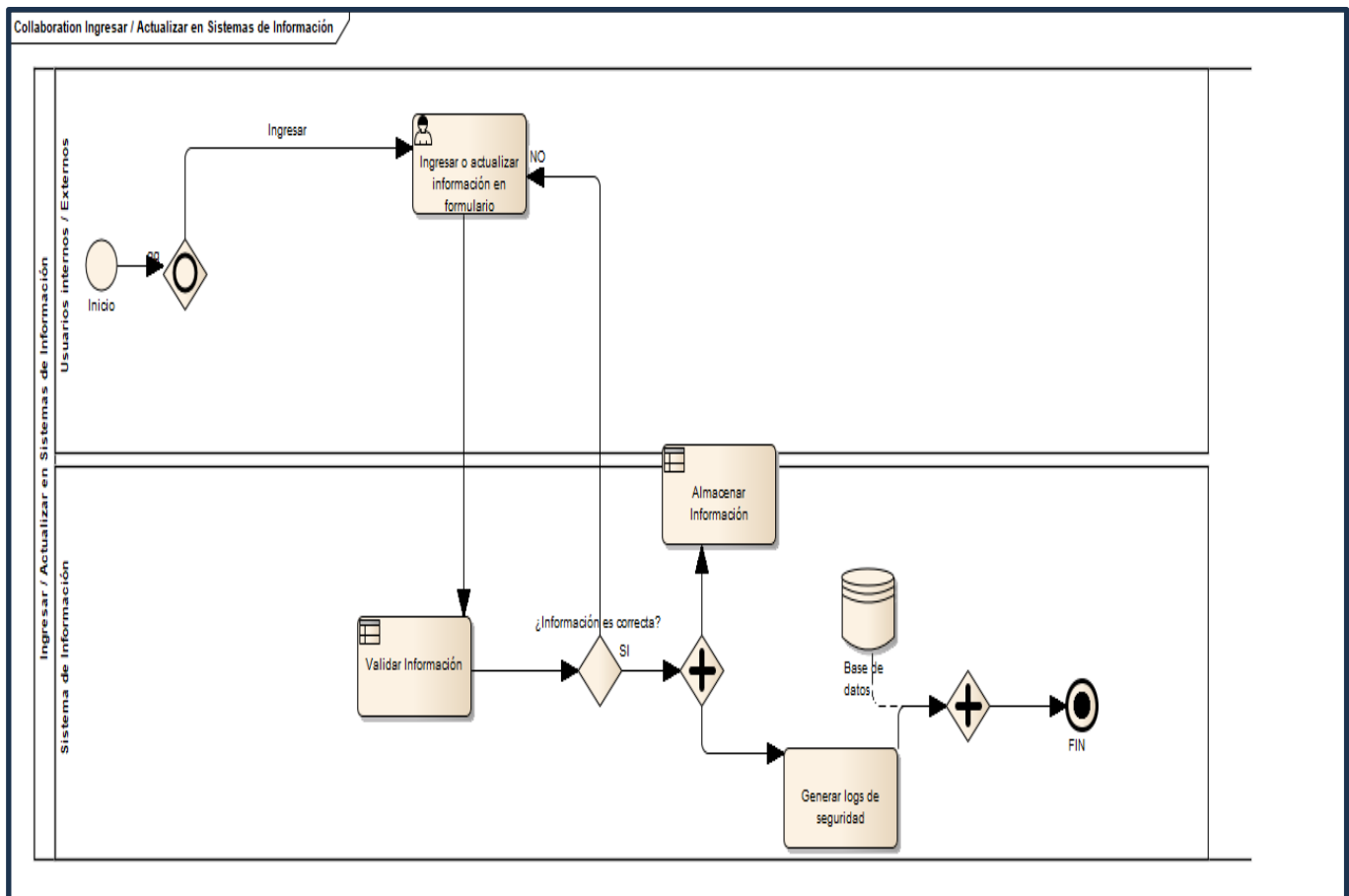
### 4.3. Fase 3 Evaluación de Estrategias

#### 4.3.1. Evaluación y selección de prioridades

Dada la amplitud y la complejidad de los documentos electrónicos o digitalizados o que se encuentran en dispositivos análogos y que deben estar disponibles a lo largo del tiempo, es esencial dar prioridad a las actividades de preservación digital de algunos documentos electrónicos considerados prioritarios. (1)

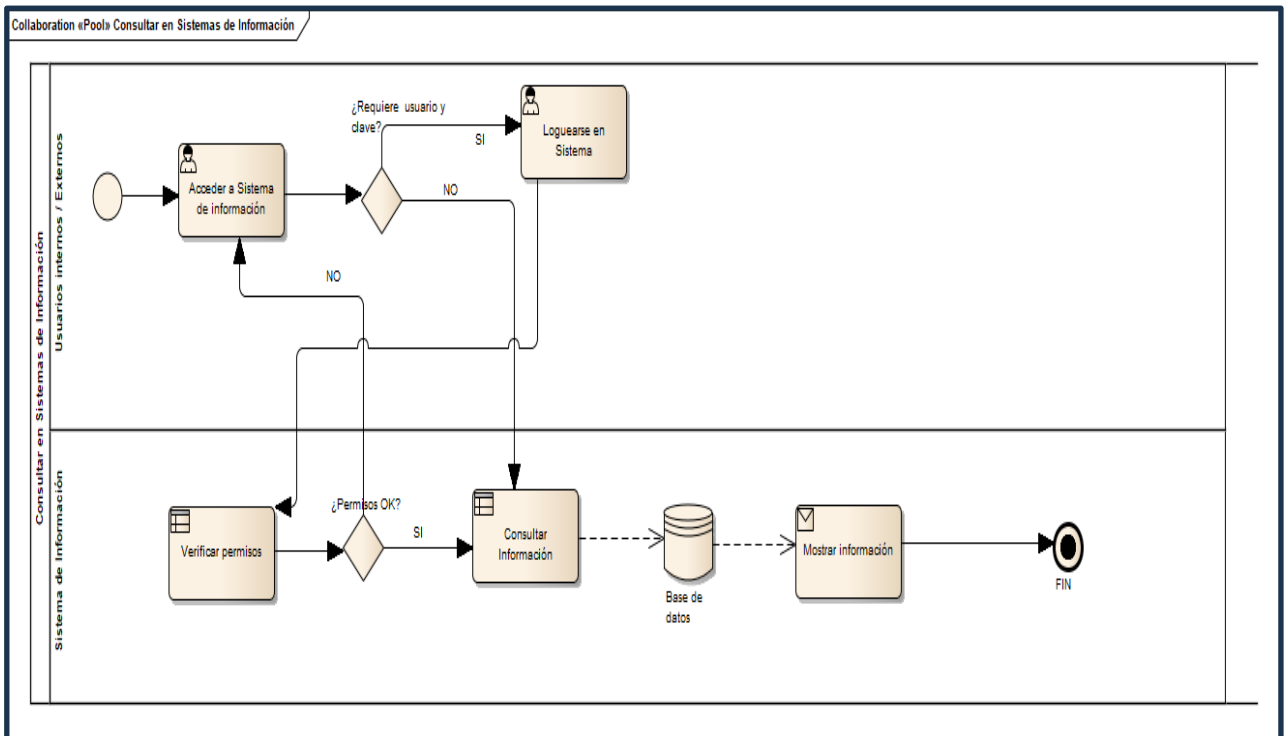
A continuación, se presentan las gráficas de los flujos de información:

##### 4.3.1.1. Ingresar Actualizar en Sistemas de Información





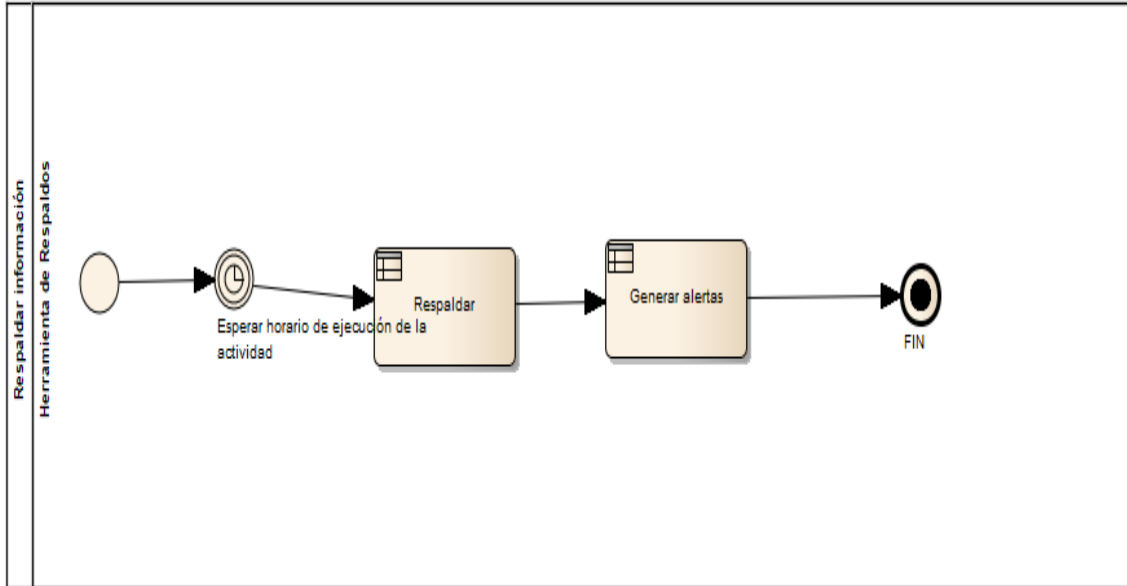
### 4.3.1.2.Consultar en Sistemas de Información



### 4.3.1.3.Respaldar Información

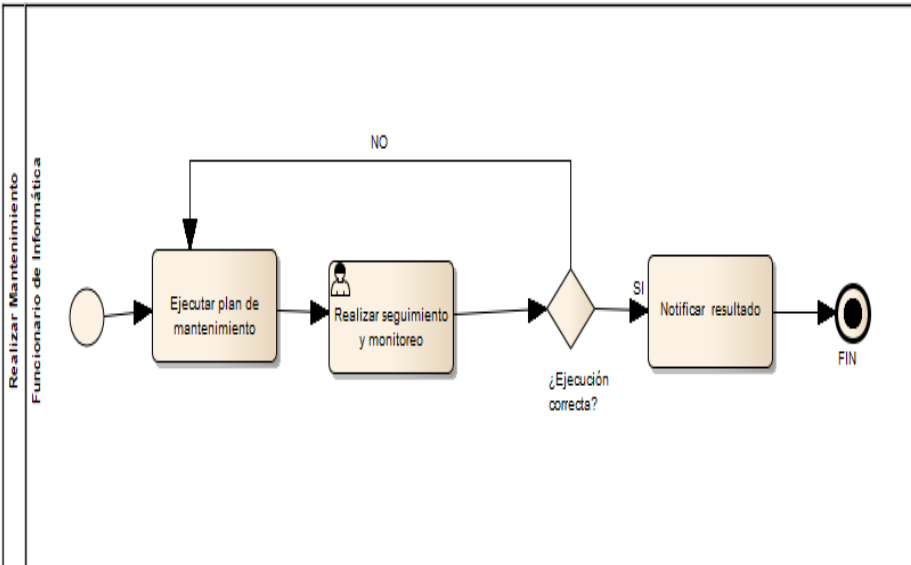


Collaboration Respaldar Información



4.3.1.4. Realizar mantenimiento

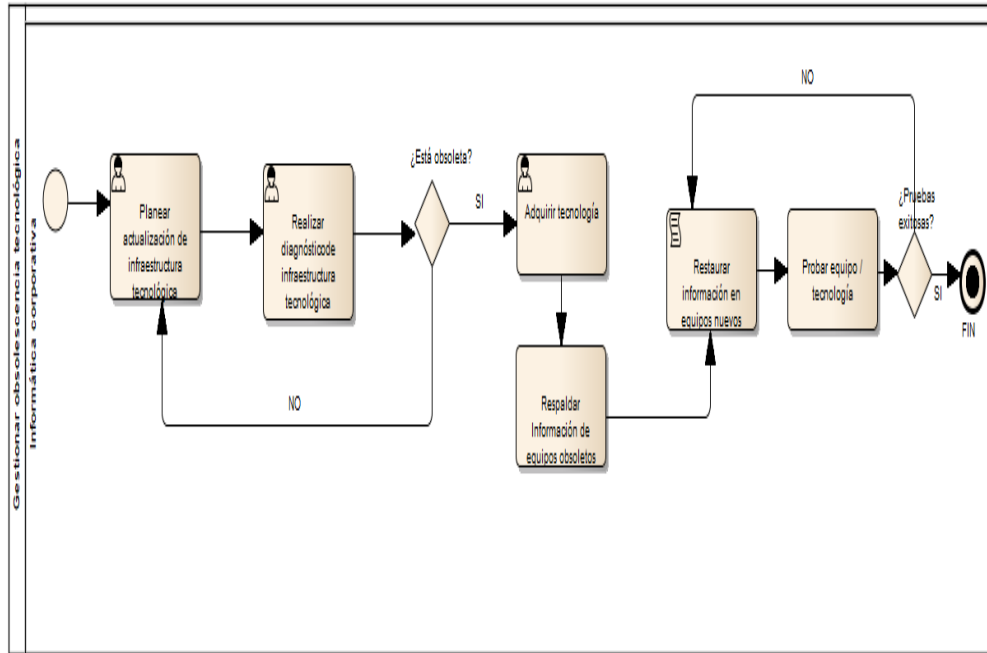
Collaboration Realizar mantenimiento



4.3.1.5. Gestionar obsolescencia tecnológica

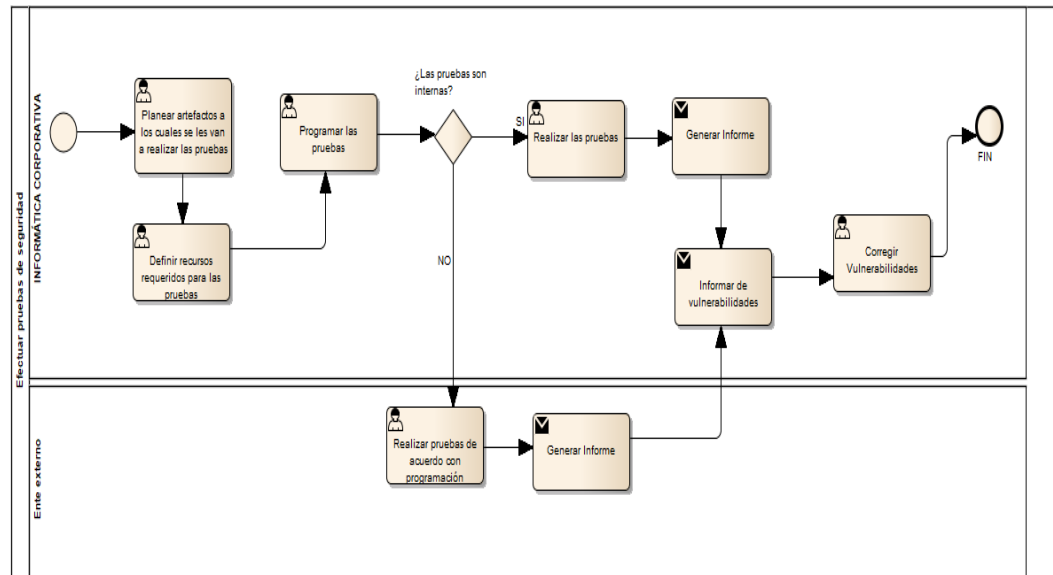


Collaboration Gestionar obsolescencia tecnológica




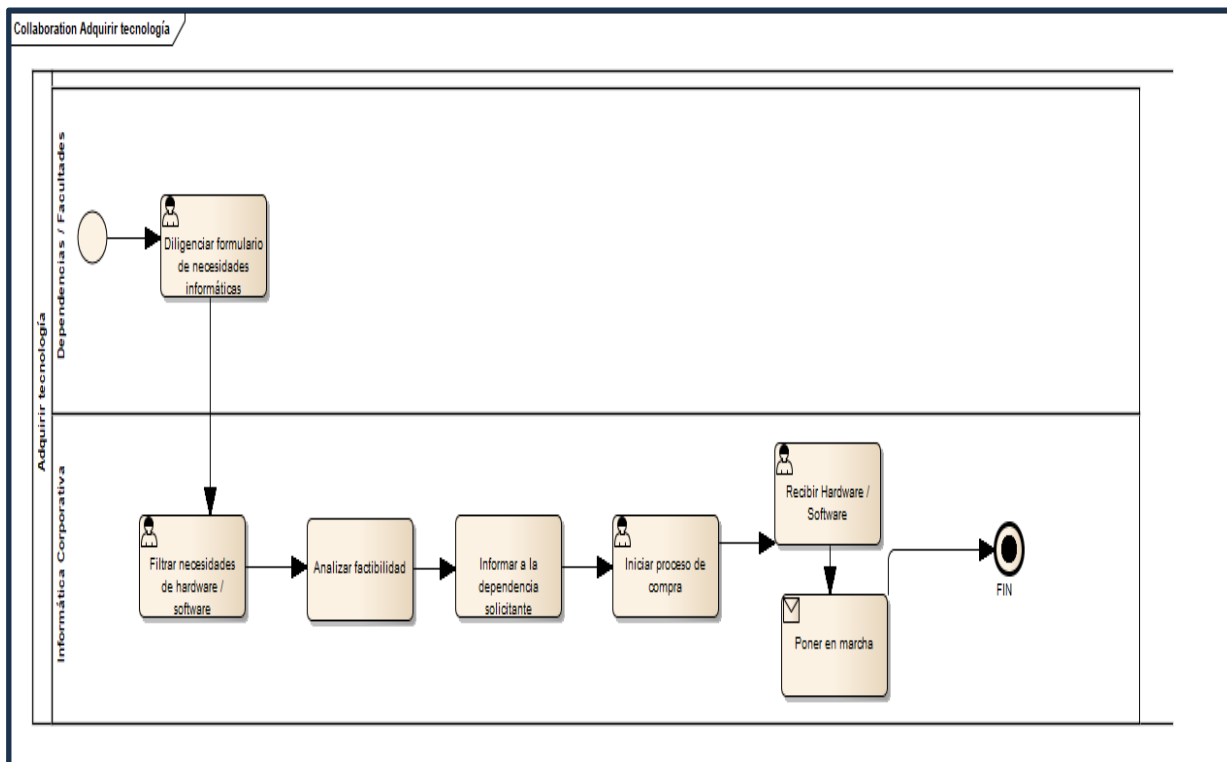
### 4.3.1.6.Efectuar pruebas de seguridad

Collaboration Efectuar pruebas de seguridad



### 4.3.1.7.Adquirir tecnología – Planeación

 POLITÉCNICO COLOMBIANO JAIME ESCALA CADAVID	<b>PLAN DE PRESERVACION DIGITAL</b>	<b>Código: ANL04</b>
		<b>Versión: 2</b>



#### 4.3.2. Caracterización de los documentos electrónicos a preservar

La caracterización, es decir: la apariencia, contenido y estructura se encuentran descritos en los siguientes programas específicos del Programa de Gestión Documental –PGD–, que se pueden consultar en el Sistema de Información “Mejoramiso” y en el micrositio de Gestión Documental de la Página Web Institucional, en el siguiente enlace:

<https://www.politecnicojic.edu.co/instrumentos-archivisticos>

- Programa De Formas Y Formularios Electrónicos
- Esquema De Metadatos Para La Gestión De Documentos Electrónicos

#### 4.3.3. Identificación y evaluación de estrategias de preservación

Para la identificación y evaluación de las estrategias de preservación digital a largo plazo en la Institución, se tienen en cuenta los siguientes criterios:

- Normalización de la estructura semántica para el nombre/renombramiento de los documentos, el cual se encuentra definido en el Programa de Documentos Electrónicos, que se encuentra publicado en la Página Web Institucional, en el siguiente enlace: <https://www.politecnicojic.edu.co/instrumentos-archivisticos>

	<b>PLAN DE PRESERVACION DIGITAL</b>	<b>Código: ANL04</b>
		<b>Versión: 2</b>


- Política de administración de riesgos definida en: <https://www.politecnicojic.edu.co/administracion-de-riesgos>
- Cumplimiento de las políticas de seguridad y privacidad de la información, tales como:
  - Las copias de seguridad se realizan de acuerdo con criticidad definida en el documento activos de información.
  - El control de acceso: por aplicación, a nivel de servidores, Sistema de archivos, Firewall.
  - Acciones preventivas: Control ante ataque de virus y hackers en concordancia con políticas de seguridad, plan de tratamiento de riesgos, plan de mantenimiento.
  - Acciones correctivas por medio del plan de contingencia.
- Instrumentos de la gestión documental a los que se les realizará un estudio para verificar viabilidad técnica y financiera, tales como: planes o actividades que podrían requerir de algún artefacto relacionado con las tecnologías de la información para garantizar la integridad, confidencialidad. Disponibilidad y accesibilidad.
- Procedimientos de preservación digital:
  - Procedimiento de identificación y análisis de series documentales a preservar
  - Procedimiento de transferencias documentales electrónicas
  - Procedimiento de administración del sistema de preservación digital:
    - Actualización de riesgos
    - Ejecución del plan de mantenimiento
    - Garantía de actualizaciones al software por parte del proveedor, con el fin de evitar pérdida de información debido a vulnerabilidades en el software.
    - Ajustes al plan de preservación
    - Evaluación al Sistema actual incluyendo medios de almacenamiento.


#### 4.3.4.Estrategias de preservación

El siguiente catálogo es basado en el anexo 1. Formatos de archivo de uso común de la Guía para la gestión de documentos y expedientes electrónicos (G.INF.07) de la Institución

##### 4.3.4.1.Normalización de formatos

FORMATO	CARACTERÍSTICA	EXTENSIÓN	ESTÁNDAR
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

 <p>POLITÉCNICO COLOMBIANO JAIME ESCALA CADAVID</p>	<b>PLAN DE PRESERVACION DIGITAL</b>		<b>Código: ANL04</b>
			<b>Versión: 2</b>
	PDF/A-1b (Subnivel b = Básico) Garantiza que el texto del documento se puede visualizar correctamente.		
	PDF/A-2a (Subnivel a = avanzado) Adicional contiene información textual o sobre la estructura lógica del documento.		
PDF/ A-2	PDF/A-2 Características adicionales que no están disponibles en formato PDF/A-1	.pdf	ISO 19005-2 ISO 32000-1
	PDF/A-2b (Subnivel b = Básico) Se cumplen todos los requisitos descritos como necesarios		
	PDF/A-2a (Subnivel a = avanzado) Adicional contiene información textual o sobre la estructura lógica del documento.		
	PDF/A-2u (Subnivel u = Unicode) Requisito adicional, todo el texto en el documento tienen equivalentes en Unicode		
PDF/A-3	PDF/A-3 Ofrece soporte para archivos incrustados.	.pdf	ISO 19005-3 ISO 32000-1
	PDF/A-3b (Subnivel b = básico) Se cumplen todos los requisitos descritos como necesarios para un PDF/A-3.		
	PDF/A-3a (Subnivel a = avanzado) etiquetado de forma que se describa y conserve la estructura lógica el orden de lectura		
XML	Es un estándar abierto, flexible y ampliamente utilizado para almacenar, publicar e intercambiar cualquier tipo de información.	.xml	W3C HTML Estándar Abierto
JPEG2000	JPEG2000 (sin pérdida) permite reducir el peso de los archivos a la mitad en comparación con las imágenes no comprimidas.	.jpg2 .jp2	ISO/IEC 15444
TIFF	TIFF (sin compresión) Archivos más grandes que un formato comprimido	.tiff	ISO 12639
Bwf	Formato de archivo que toma la estructura de archivos WAVE existente y añade metadatos adicionales	.bwf	EBU - TECH 3285
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
GZIP	Formato de compresión de datos	.gz	RFC 1952 Estándar Abierto
SQL	Structured Query Language,	.sql	ISO 9075-1

 POLITÉCNICO COLOMBIANO JAIME ESCALA CADAVID	<b>PLAN DE PRESERVACION DIGITAL</b>			<b>Código: ANL04</b>
				<b>Versión: 2</b>
	de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones en ella			
MBOX	Formato utilizado para almacenar conjuntos de correos electrónicos.	mbox, .mbx	N/A	

#### 4.3.4.2.Migración

En la Norma Técnica Colombiana ISO 13008, la migración se define como el proceso de mover documentos electrónicos de una configuración de hardware o software a otra sin cambiar el formato. (1)

La migración de la información puede llegar a ser una necesidad debida a cambios en los requerimientos de hardware y/o software. A continuación, se detallan algunos puntos que la Institución considera para tal fin:

- Necesidad justificada debido a:
  - Actualizaciones a nivel de hardware:
    - Se requiere contar con la infraestructura necesaria requerida sin afectar la integridad, confidencialidad y disponibilidad de la información ya existente.
    - Respaldo de la información en nuevos medios con las respectivas pruebas de restauración en laboratorio.
    - El nuevo Hardware debe soportar el Sistema de Información / Motor de base de datos / repositorio
    - La configuración del Sistema debe cumplir con estándares de seguridad.
    - El proceso lo debe realizar personal experto
    - El hardware deberá estar en una zona protegida.
  - Software que no cumple con los requerimientos mínimos
    - Los requerimientos de norma ameritan cambio de versión del software
    - El software presenta falencias graves en cuanto a requisitos mínimos funcionales y/o no funcionales.
  - Nueva versión del Sistema con mejoras relevantes al proceso y/o a la seguridad.
    - El software presenta vulnerabilidades en su seguridad y requiere parches o actualizaciones.

 POLITÉCNICO COLOMBIANO JAIME ESCALA CADAVID	<b>PLAN DE PRESERVACION DIGITAL</b>	<b>Código: ANL04</b>
		<b>Versión: 2</b>

- El software ha cambiado de versión y tiene mejoras significativas para una mayor efectividad en la ejecución del proceso.
- Sistema operativo no soportado por el fabricante.
  - El Sistema operativo en el cual está alojada la aplicación deja de recibir soporte por parte del fabricante dejando huecos en la seguridad sin ser parchados exponiendo la aplicación a vulnerabilidades y posible afectación en cuanto a integridad, confidencialidad y disponibilidad.
  - Se debe revisar que la aplicación sea compatible con Sistemas Operativos más actualizados y en caso de incompatibilidad toma de decisiones en cuanto al riesgo de acuerdo con plan de tratamiento del riesgo (<http://surl.li/frkvo>) y plan estratégico de las tecnologías de la información (<http://surl.li/rpgwle>)
- Cambio de motor de Base de datos:
  - En el caso de motor de BD original basado en SQL y motor de BD destino SQL, existen métodos que permiten importar los datos de una forma más fluida por la compatibilidad. Es importante que el modelo de base de datos, su diccionario no se vea afectado en el cambio para evitar pérdida de integridad y la nueva base de datos deberá tener la seguridad requerida para mantener la confidencialidad de la información.
- Para la migración se deberá tener el soporte financiero que permita acceder a los recursos requeridos:
  - Disponibilidad presupuestal
  - Estudios previos
  - Solicitud de concepto
  - Solicitud de certificado de disponibilidad presupuestal (CDP)
  - Sometimiento a aprobación en comités internos
  - Adquisición del artefacto

La institución propenderá en lo posible para que en el tipo de migración utilizado no exista “*cambio en el empaquetado de la información, la información del contenido ni la Información de la Descripción de Preservación. Los bits utilizados para representar estos objetos de información son preservados en la transferencia en la misma o un nuevo medio*”. (1)

#### **4.3.4.3. Conversión**

 <p>POLITÉCNICO COLOMBIANO JAIME ESCALA CADAVID</p>	<h2>PLAN DE PRESERVACION DIGITAL</h2>	<p><b>Código: ANL04</b></p> <hr/> <p><b>Versión: 2</b></p>
---	---------------------------------------	--

La conversión de un formato a otro puede deberse a obsolescencia o simplemente necesidad de cambio. En todo caso el formato seleccionado como destino deberá tener por lo menos una compatibilidad a largo plazo como PDF/A

- La conversión a formatos abiertos asegura que los documentos sean accesibles en el futuro, independientemente de la evolución de las tecnologías y software. Esto facilita el acceso a la información por parte de la comunidad institucional en el largo plazo.
- Al utilizar formatos estandarizados, se mejora la compatibilidad entre diferentes sistemas y plataformas. Esto es especialmente importante en un entorno educativo donde se utilizan múltiples herramientas y aplicaciones.
- La conversión a formatos abiertos y ampliamente aceptados evita la dependencia de software propietario que puede volverse obsoleto o dejar de ser soportado, garantizando que los recursos digitales se mantengan utilizables.

Para aplicar la estrategia de conversión de formatos en la institución, se pueden seguir los siguientes pasos:

- ✓ Evaluación de Formatos Existentes:
  - Realizar un inventario de todos los documentos y recursos digitales que la institución posee, identificando los formatos actuales. Esto incluye documentos de texto, presentaciones, imágenes, videos y otros tipos de archivos.
- ✓ Selección de Formatos Abiertos:
  - Investigar y seleccionar formatos abiertos y estandarizados que sean adecuados para cada tipo de recurso. Por ejemplo:
    - Documentos de texto: Convertir de DOCX a ODT.
    - Imágenes: Convertir de JPEG a PNG o TIFF.
    - Presentaciones: Convertir de PPTX a ODP.
- ✓ Implementación de Herramientas de Conversión:
  - Utilizar software de conversión que permita realizar la transformación de manera eficiente. Esto puede incluir herramientas en línea, software de escritorio o scripts automatizados.
  - Capacitar al personal en el uso de estas herramientas para que puedan realizar la conversión de manera efectiva.
  - Búsqueda de herramientas de conversión masivas de uso libre.
- ✓ Documentación del Proceso:

 <p>POLITÉCNICO COLOMBIANO JAIME ESCALA CADAVID</p>	<p><b>PLAN DE PRESERVACION DIGITAL</b></p>	<p><b>Código: ANL04</b></p>
		<p><b>Versión: 2</b></p>

- Crear un manual o guía que detalle el proceso de conversión, incluyendo los pasos a seguir, las herramientas recomendadas y las mejores prácticas a aplicar.
- ✓ **Monitoreo y Mantenimiento:**
  - Establecer un sistema de revisión periódica para asegurarse de que los formatos de archivo se mantengan actualizados y que se apliquen las conversiones cuando se añadan nuevos recursos digitales.

#### **4.3.4.4.Refreshing**

El proceso de copiar cierto contenido digital desde un medio digital hacia otro (incluye copiado al mismo tipo de medio). También se conoce como “refrescado”. (3). Según AGN, “No preserva los datos, pero es un paso imprescindible para garantizar el acceso a aquellos” (1).

A continuación, algunos pasos que se podrían considerar en esta técnica de preservación:

- ✓ **Evaluación de Activos Digitales:** Realizar un inventario de todos los activos digitales, incluyendo documentos, imágenes, videos, bases de datos y otros recursos. Identificar el formato, el medio de almacenamiento actual y la antigüedad de cada recurso.
- ✓ **Establecimiento de un Cronograma de Refreshing:** Incluir en el cronograma la revisión de los formatos y la actualización de los sistemas de almacenamiento.
  - ✓ **Selección de Nuevos Medios de Almacenamiento:** Elegir medios de almacenamiento modernos y confiables y asegurarse de que los nuevos medios sean compatibles con los formatos de archivo existentes.
- ✓ **Migración de Datos:** Al transferir los datos desde los medios antiguos a los nuevos, se hace necesario:
  - Realizar copias de seguridad antes de la migración.
  - Usar herramientas de migración que verifiquen la integridad.
- ✓ **Verificación y Validación:** Después de la migración, realizar pruebas para verificar que todos los archivos se han transferido correctamente y que son accesibles. Se recomienda realizar una prueba a una muestra de datos.
- ✓ **Documentación del Proceso:** Registrar el proceso de Refreshing, incluyendo la fecha de la migración, los medios utilizados, los formatos de archivo y cualquier problema encontrado durante el proceso. Toda esta información podría servir en un futuro hace parte de las lecciones aprendidas y gestión del conocimiento.

 <p>POLITÉCNICO COLOMBIANO JAIME ESCALA CADAVID</p>	<p><b>PLAN DE PRESERVACION DIGITAL</b></p>	<p><b>Código: ANL04</b></p> <hr/> <p><b>Versión: 2</b></p>
---	--	--

- ✓ **Concienciación y Capacitación del Personal:** Capacitar al personal sobre la importancia del Refreshing y cómo realizarlo correctamente. Esto incluye la identificación de activos digitales que necesitan ser refrescados y los procedimientos para llevar a cabo la migración.
- ✓ **Monitoreo Continuo:** Establecer un sistema de monitoreo que permita detectar cuándo un medio de almacenamiento se está volviendo obsoleto, para planificar el próximo ciclo de Refreshing.

En resumen, el "Refreshing" va a permitir:

- **Prevención de Pérdida de Datos:** Al actualizar regularmente los medios de almacenamiento y los formatos, se reduce el riesgo de pérdida de datos debido a la degradación de los soportes.
- **Mejora en el Acceso y Uso:** Los datos actualizados están en formatos y medios modernos, lo que puede mejorar la velocidad de acceso y la compatibilidad con las herramientas actuales.
- **Aumento de la Vida Útil de los Datos:** El proceso de Refreshing ayuda a extender la vida útil de los recursos digitales, asegurando que continúen siendo utilizables a lo largo del tiempo.

La desventaja principal del Refreshing es que puede requerir tiempo, personal y recursos financieros. La migración de grandes cantidades de datos puede ser laboriosa y costosa, especialmente si se realizan auditorías y verificaciones rigurosas.

Al implementar la técnica de Refreshing de manera sistemática y planificada, la institución puede garantizar la sostenibilidad y accesibilidad de sus activos digitales a largo plazo.

#### **4.3.4.5. Emulación**

Técnica informática que consiste en la reproducción, en equipos y software actuales, lo más exacta posible de programas y/o equipos obsoletos para acceder a la información contenida en ellos. (3). El software y equipos utilizados deberán garantizar la integridad, confidencialidad y disponibilidad de la información.

Esta técnica puede ofrecer una alternativa viable para asegurar el acceso digital de la información en el futuro. Uno de los beneficios comparado con la migración es que el dato original no necesita ser alterado en ningún momento. Es la emulación del ambiente computacional la que cambiará con el tiempo. (4)

Otra ventaja de implementar la emulación es su posible eficiencia. Una vez el dato es archivado con la metadata y softwares apropiados, no se requiere otra acción excepto el Refreshing hasta que se

 POLITÉCNICO COLOMBIANO JAIME ESCALA CADAVID	<b>PLAN DE PRESERVACION DIGITAL</b>	<b>Código: ANL04</b>
		<b>Versión: 2</b>

requiera. (4)

#### **4.3.4.6. Características mínimas de una plataforma de preservación digital**

Las características mínimas de la plataforma de preservación digital que requiere la institución deberán garantizar la integridad, accesibilidad y durabilidad de los recursos digitales a lo largo del tiempo:

- ✓ **Compatibilidad de Formatos:** Capacidad para gestionar y almacenar una variedad de formatos de archivo digitales, incluyendo documentos, imágenes, audio y video.
- ✓ **Metadatos:** Implementación de estándares de metadatos que faciliten la identificación, descripción y gestión de los recursos digitales.
- ✓ **Integridad de los Datos:** Mecanismos para verificar la integridad de los datos, como el uso de sumas de verificación (checksums) y controles de versión.
- ✓ **Accesibilidad:** Garantizar que los recursos sean accesibles a los usuarios autorizados, con interfaces que permitan la búsqueda y recuperación eficiente de la información.
- ✓ **Seguridad:** Provisión de medidas de seguridad para proteger los datos contra el acceso no autorizado, la pérdida y la corrupción, incluyendo copias de seguridad y recuperación ante desastres.
- ✓ **Escalabilidad:** Capacidad de la plataforma para crecer y adaptarse a un aumento en la cantidad de datos y usuarios sin comprometer el rendimiento.
- ✓ **Interoperabilidad:** Posibilidad de interactuar con otras plataformas y sistemas, lo que facilita el intercambio de datos y la colaboración.
- ✓ **Sostenibilidad:** Estrategias para asegurar la continuidad de la plataforma a largo plazo, incluyendo el mantenimiento y la actualización de la tecnología.
- ✓ **Documentación y Soporte:** Disponibilidad de documentación clara y recursos de soporte para usuarios y administradores de la plataforma.
- ✓ **Cumplimiento Normativo:** Asegurarse de que la plataforma cumpla con las regulaciones y estándares éticos relevantes en materia de preservación y gestión de datos.

	<b>PLAN DE PRESERVACION DIGITAL</b>	Código: ANL04
		Versión: 2

Estas características son esenciales para garantizar que los activos digitales sean preservados de manera efectiva y estén disponibles para las generaciones futuras.

#### 4.3.5. Evaluación de las estrategias de preservación

Las siguientes estrategias, junto con sus riesgos y actividades específicas, pueden ayudar a asegurar la efectividad de la preservación digital a largo plazo.

<b>Estrategia # 1</b>	
<b>Nombre</b>	Replicación y Almacenamiento en Múltiples Ubicaciones
<b>Riesgos</b>	<ul style="list-style-type: none"> <li>- Dependencia de la infraestructura de terceros.</li> <li>- Costos asociados al almacenamiento externo.</li> <li>- Dificultades en la sincronización de datos.</li> </ul>
<b>Justificación</b>	Mantener copias en diferentes ubicaciones reduce el riesgo de pérdida de datos debido a desastres locales o fallos en el hardware.
<b>Actividades</b>	<ol style="list-style-type: none"> <li>1. Establecer copias de seguridad automáticas en la nube y en servidores locales.</li> <li>2. Realizar auditorías periódicas para asegurar que todas las copias estén actualizadas y sean accesibles.</li> <li>3. Documentar y probar los procedimientos de recuperación de datos.</li> </ol>
<b>Responsable</b>	Informática Corporativa

<b>Estrategia # 2</b>	
<b>Nombre</b>	Establecer formatos abiertos y estándares adecuados
<b>Riesgos</b>	<ul style="list-style-type: none"> <li>- Posibles limitaciones en la funcionalidad de ciertos formatos.</li> <li>- Pérdida de calidad al convertir archivos a formatos abiertos.</li> </ul>
<b>Justificación</b>	Los formatos abiertos son más sostenibles a largo plazo, ya que no dependen de un proveedor específico y son más accesibles para futuras tecnologías.
<b>Actividades</b>	<ol style="list-style-type: none"> <li>1. Evaluar periódicamente los formatos de archivo utilizados y convertirlos a formatos abiertos si es necesario.</li> <li>2. Crear un inventario de formatos de archivo y su estado de preservación.</li> </ol>


	<b>PLAN DE PRESERVACION DIGITAL</b>	<b>Código: ANL04</b>
		<b>Versión: 2</b>

	3. Establecer políticas de selección de formatos para nuevos activos digitales.
<b>Responsable</b>	Coordinación de Archivo y correspondencia

<b>Estrategia #</b>	<b>3</b>
<b>Nombre</b>	Mantenimiento de Metadatos Ricos y Estandarizados
<b>Riesgos</b>	- Complejidad en la creación y mantenimiento de metadatos. - Riesgo de obsolescencia si los estándares cambian.
<b>Justificación</b>	Los metadatos adecuados facilitan la búsqueda, identificación y uso de los recursos digitales, además de asegurar su contexto y significado.
<b>Actividades</b>	1. Identificar y documentar los metadatos relevantes 2. Capacitar al personal en la importancia de los metadatos y en su correcta aplicación. 3. Realizar revisiones periódicas de los metadatos para asegurarse de que sean precisos y completos.
<b>Responsable</b>	Coordinación de Archivo y correspondencia, Informática Corporativa

<b>Estrategia #</b>	<b>4</b>
<b>Nombre</b>	Seguimientos anuales del plan de preservación
<b>Riesgos</b>	- Recursos limitados para llevar a cabo el seguimiento. - Posibilidad de pasar por alto problemas críticos.
<b>Justificación</b>	El seguimiento ayuda a identificar problemas potenciales en las estrategias de preservación y a garantizar que se cumplan las políticas establecidas.
<b>Actividades</b>	1. Realizar seguimientos anuales del sistema de preservación y de los activos digitales. 2. Identificar acciones de mejora e implementarlas. 3. Documentar los hallazgos y crear un plan de acción para abordar cualquier problema identificado.
<b>Responsable</b>	Coordinación de Archivo y correspondencia, Informática Corporativa

<b>Estrategia #</b>	<b>5</b>
<b>Nombre</b>	Educación y Capacitación Continua del Personal

	<b>PLAN DE PRESERVACION DIGITAL</b>	<b>Código: ANL04</b>
		<b>Versión: 2</b>
<b>Riesgos</b>	<ul style="list-style-type: none"> <li>- Resistencia al cambio por parte del personal.</li> <li>- Falta de recursos para capacitación continua.</li> </ul>	
<b>Justificación</b>	Un personal bien informado y capacitado es crucial para la implementación efectiva de las estrategias de preservación y para adaptarse a nuevas tecnologías y prácticas.	
<b>Actividades</b>	<ol style="list-style-type: none"> <li>1. Desarrollar un programa de capacitación regular sobre preservación digital y nuevas tecnologías.</li> <li>2. Crear materiales de referencia y guías para el personal sobre mejores prácticas en preservación digital.</li> <li>3. Fomentar la participación en conferencias y talleres relacionados con la preservación digital.</li> </ol>	
<b>Responsable</b>	Coordinación de Archivo y correspondencia, Informática Corporativa	

<b>Estrategia #</b>	<b>6</b>
<b>Nombre</b>	Migración
<b>Riesgos</b>	<ul style="list-style-type: none"> <li>- Pérdida de datos durante el proceso de transferencia.</li> <li>- Alteración involuntaria de la información original.</li> </ul>
<b>Justificación</b>	Obsolescencia tecnológica, cambios en la necesidad del software / hardware
<b>Actividades</b>	<ol style="list-style-type: none"> <li>1. Realizar copias de seguridad completas de todos los datos antes de iniciar el proceso de migración, asegurando que exista una forma de recuperar la información en caso de errores o fallos.</li> <li>2. Validar la integridad de los archivos antes y después de la migración mediante la verificación de checksums u otras técnicas de verificación para garantizar que no se haya producido ningún cambio no deseado en los datos.</li> <li>3. Documentar detalladamente el proceso de migración, incluyendo los pasos realizados, las decisiones tomadas y cualquier problema encontrado, para facilitar la reproducibilidad y el seguimiento de la migración en el futuro.</li> </ol>
<b>Responsable</b>	Coordinación de Archivo y correspondencia, Informática Corporativa

	<b>PLAN DE PRESERVACION DIGITAL</b>	<b>Código: ANL04</b>
		<b>Versión: 2</b>

<b>Estrategia #</b>	<b>7</b>
<b>Nombre</b>	Archivamiento de medios sociales
<b>Riesgos</b>	Posibilidad de que las plataformas de medios sociales cambien sus políticas de privacidad o de funcionamiento, lo que podría afectar la disponibilidad de los datos históricos, y el riesgo de que la información almacenada en medios sociales se vea comprometida por ciberataques o pérdida de acceso a las cuentas.
<b>Justificación</b>	Es importante tener un plan de archivamiento de medios sociales para preservar la información relevante, conversaciones, interacciones y contenido compartido en estas plataformas. Esto permite documentar la historia y evolución de una organización o marca en el entorno digital y facilita la gestión de la reputación online.
<b>Actividades</b>	<p>1. Identificar las plataformas y cuentas de medios sociales que contienen información relevante para la organización, y establecer un proceso de captura y almacenamiento periódico de estos datos, considerando la normativa vigente en cuanto a protección de datos.</p> <p>2. Implementar herramientas especializadas de archivamiento de medios sociales que permitan capturar, gestionar y preservar de manera estructurada y segura la información proveniente de diferentes plataformas y redes sociales.</p> <p>3. Definir políticas internas de retención de datos para los archivos de medios sociales, determinando qué información debe ser conservada, por cuánto tiempo y quién tiene acceso a ella, garantizando la integridad y disponibilidad de la información a lo largo del tiempo.</p>
<b>Responsable</b>	Coordinación de archivo y correspondencia, Oficina Asesora de comunicaciones, Informática Corporativa.

#### 4.3.6. Borrado Digital Seguro

La gestión de la información en el entorno digital ha alcanzado una complejidad sin precedentes,

	<b>PLAN DE PRESERVACION DIGITAL</b>	<b>Código: ANL04</b>
		<b>Versión: 2</b>

donde la capacidad de almacenar datos se ha vuelto tan crítica como la de eliminarlos de forma segura. A menudo, existe una peligrosa confusión entre la eliminación superficial de un archivo y su destrucción definitiva. Esta falta de entendimiento es la causa fundamental de numerosas filtraciones de datos, lo que expone a individuos y organizaciones a riesgos significativos. Este punto explora la naturaleza del borrado digital seguro, diferenciándolo de los métodos tradicionales y estableciendo un marco estratégico para su implementación efectiva.

#### 4.3.6.1. Eliminación Lógica

Cuando un usuario elimina un archivo de manera convencional, como al arrastrarlo a la papelera de reciclaje y vaciarla, el sistema operativo no borra los datos en sí mismos. En cambio, simplemente elimina la referencia del archivo del índice de almacenamiento del disco. Este acto, conocido como eliminación lógica, simplemente marca el espacio ocupado por el archivo como disponible para ser sobrescrito por nuevos datos. Sin embargo, la información original permanece en el disco y puede ser restaurada con relativa facilidad utilizando herramientas especializadas de recuperación de datos.

El formateo de un disco, ya sea en su modalidad rápida o completa, tampoco garantiza la destrucción total de la información. El formateo rápido simplemente elimina la estructura de archivos y los punteros, dejando los datos intactos y fácilmente recuperables con software forense. Aunque un formateo completo puede sobrescribir algunos sectores del disco, los datos no se eliminan de forma segura, y la información más sensible podría seguir siendo accesible para atacantes o analistas forenses con las herramientas adecuadas. Esta discrepancia entre la percepción de la seguridad y la realidad técnica constituye el origen de la mayoría de las filtraciones de datos por borrado inadecuado. La confianza errónea en estos métodos convencionales crea una peligrosa vulnerabilidad que, como se detalla más adelante, tiene graves repercusiones.

#### 4.3.6.2. Definición y Principios Fundamentales del Borrado Digital Seguro

En contraste con los métodos de eliminación superficial, el borrado digital seguro es un proceso técnico y certificado diseñado para eliminar datos de forma definitiva, minimizando la probabilidad de su recuperación. No se trata de un simple comando, sino de una medida de seguridad que establece métodos y técnicas robustas para la destrucción de la información.

De acuerdo con los estándares internacionales en la materia, el borrado seguro se rige por tres principios fundamentales:

- **Irreversibilidad:** El proceso debe garantizar que la información no pueda ser recuperada por ningún medio, ni siquiera con técnicas forenses avanzadas. Esto asegura la confidencialidad de los datos a lo largo de su ciclo de vida y después de su disposición.
- **Seguridad y Confidencialidad:** Durante el proceso de borrado, los medios de almacenamiento deben ser tratados con el mismo nivel de seguridad con el que se manejaron a lo largo de su existencia. Esto implica proteger los dispositivos de accesos no autorizados antes, durante y después de la destrucción de los datos.

 <p>POLITÉCNICO COLOMBIANO JAIME ESCALA CADAVID</p>	<p><b>PLAN DE PRESERVACION DIGITAL</b></p>	<p><b>Código: ANL04</b></p>
		<p><b>Versión: 2</b></p>

- **Favorable al Medio Ambiente:** Un método de borrado seguro debe ser diseñado para producir el mínimo de emisiones y desperdicios, promoviendo la reutilización y el reciclaje de los dispositivos siempre que sea posible. Este principio subraya la necesidad de que las políticas de seguridad de la información consideren también la responsabilidad corporativa y ambiental.

#### 4.3.6.3. Riesgos de una Gestión Inadecuada de Datos

La principal consecuencia de no borrar los datos de forma segura es la fuga de información confidencial o personal. Al desechar, vender o donar un dispositivo de almacenamiento sin una destrucción adecuada de los datos, se corre el riesgo de que información sensible, como datos de clientes, registros financieros, propiedad intelectual o información de autenticación, caiga en manos de terceros malintencionados.

Además, esta exposición de datos puede desencadenar daños secundarios significativos, como el robo de identidad. La información de cuentas restaurada puede ser utilizada para suplantación de identidad, lo que resulta en graves pérdidas financieras tanto para la persona como para la organización afectada. Las fugas de información tienen un impacto directo en la credibilidad y la reputación, por ello, la confianza de usuarios y partes interesadas puede verse seriamente dañada, afectando la imagen pública y las relaciones de negocio a largo plazo.

#### 4.3.6.4. Casos de Uso Críticos para el Borrado Digital Seguro

La necesidad de un borrado digital seguro se manifiesta en diversas situaciones críticas a lo largo del ciclo de vida de los activos digitales:

- **Fin del Ciclo de Vida de un Equipo:** Cuando un equipo, como un servidor, disco duro o unidad SSD, llega al final de su vida útil y se planea desechar, donar, revender o reciclar, el borrado seguro es un paso obligatorio para garantizar que los datos confidenciales no sean accesibles para nuevos usuarios.
- **Desvinculación de Empleados:** Al terminar la relación laboral con un empleado que ha tenido acceso a información confidencial, es imperativo realizar un borrado seguro de los dispositivos que utilizó para proteger los activos de la Institución.
- **Migraciones de Infraestructura de TI:** Durante la renovación de activos tecnológicos o la transición a nuevas plataformas, como la nube, el borrado seguro de los dispositivos antiguos es crucial para la seguridad de la información.
- **Gestión de eliminación de Documentos de Archivos que ya han cumplido su tiempo:** El borrado periódico de datos obsoletos no solo es una medida de seguridad, sino también una práctica de optimización que libera espacio de almacenamiento y mejora la eficiencia de los procesos operativos, así como la aplicación de Instrumentos Archivísticos como las Tablas de Retención documental y Tablas de Valoración Documental.

#### 4. Métodos Técnicos de Borrado Digital Seguro por Tipo de Medio

No existe una solución única para el borrado seguro; el método óptimo depende en gran medida del tipo de medio de almacenamiento y del nivel de confidencialidad de los datos. Los métodos se dividen

 <p>POLITÉCNICO COLOMBIANO JAIME ESCALA CADAVID</p>	<p><b>PLAN DE PRESERVACION DIGITAL</b></p>	<p><b>Código: ANL04</b></p> <hr/> <p><b>Versión: 2</b></p>
---	--	--

en dos categorías principales: lógicos (basados en software) y físicos (basados en hardware).

#### **4.3.6.5. Métodos Lógicos (Basados en Software)**

- **La Sobrescritura de Datos**

La sobrescritura es la técnica de borrado digital más conocida, que consiste en reemplazar los datos originales en un disco con patrones de ceros, unos o datos aleatorios. Este método es especialmente eficaz en los discos duros magnéticos (HDD), donde se utiliza un número de pasadas (una o varias) para garantizar que los datos antiguos sean indetectables. Una de sus mayores ventajas es que permite reutilizar el dispositivo sin causarle daño físico.

No obstante, la sobrescritura presenta un desafío único en las unidades de estado sólido (SSD). Debido a la forma en que los SSD gestionan los datos mediante un controlador de memoria flash, un comando de sobrescritura del sistema operativo no necesariamente se aplica a todas las instancias de los datos. El controlador puede traducir el comando de forma que no se sobrescriban todas las celdas de memoria, dejando datos residuales.

- **El Borrado Criptográfico (CE)**

El borrado criptográfico ha surgido como el método preferido para las unidades SSD y otros dispositivos modernos que utilizan cifrado de datos. En lugar de sobrescribir físicamente los datos, esta técnica se centra en la destrucción de las claves de cifrado que los hacen legibles. Al eliminar la clave criptográfica, los datos cifrados se vuelven irre recuperables, lo que hace que el proceso sea rápido y eficiente, permitiendo la reutilización del dispositivo.

Sin embargo, confiar exclusivamente en este método puede presentar un riesgo sutil. Algunos restablecimientos de fábrica en dispositivos móviles y SSD solo eliminan la clave de cifrado, dejando físicamente los datos en el almacenamiento. Esto crea una vulnerabilidad potencial: un atacante con recursos suficientes y técnicas forenses avanzadas podría, en teoría, intentar reconstruir los datos si la implementación del borrado de claves no es robusta o si el firmware tiene fallos. Por ello, para los datos de altísima sensibilidad, la mejor práctica puede ser combinar el borrado criptográfico con una sobrescritura física de múltiples pasadas, asegurando así una defensa en profundidad que mitigue cualquier posibilidad de recuperación.

#### **4.3.6.6. Métodos Físicos (Basados en Hardware)**

- **Desmagnetización**

La desmagnetización es un método físico que utiliza un potente campo magnético para alterar los dominios magnéticos de un medio de almacenamiento, haciendo que los datos sean ilegibles. Es un proceso rápido y efectivo, ideal para la destrucción masiva de datos en medios magnéticos como discos duros y cintas de respaldo. Es importante destacar que este método es completamente ineficaz para las unidades de estado sólido y otros dispositivos de memoria flash, ya que no dependen de la tecnología magnética para almacenar la información.

 POLITÉCNICO COLOMBIANO JAIME ESCALA CADAVID	<b>PLAN DE PRESERVACION DIGITAL</b>	Código: ANL04
		Versión: 2

- **Destrucción Física**

La destrucción física es considerada el método más seguro y definitivo para el borrado de datos. Implica dañar el dispositivo de manera irreversible, haciéndolo inoperable y garantizando que los datos no puedan ser recuperados. Las técnicas varían desde la trituración o pulverización, que convierte el disco en pequeñas partículas, hasta la desintegración, la abrasión, la fundición o la incineración. Aunque proporciona la máxima garantía de seguridad, la destrucción física tiene el inconveniente de que hace que el dispositivo sea completamente inutilizable, lo que conlleva un costo económico y un impacto ambiental significativo al generar desechos electrónicos.

**Tabla 4 Métodos de Borrado por Tipo de Dispositivo y Nivel de Sensibilidad**

Tipo de Dispositivo	Nivel de Sensibilidad de los Datos	Método Recomendado	Ventajas	Desventajas
HDD (Disco Duro)	Bajo (archivos personales, no confidenciales)	Sobreescritura de una sola pasada (NIST Clear)	Permite la reutilización, bajo costo.	Riesgo de recuperación con herramientas avanzadas.
HDD (Disco Duro)	Medio (datos corporativos)	Sobreescritura de múltiples pasadas (DoD 5220.22-M)	Fiable, ampliamente reconocido.	Lento, no apto para SSD.
HDD (Disco Duro)	Alto (datos clasificados)	Desmagnetización o Destrucción Física	Máxima seguridad garantizada.	Destruye el dispositivo, impacto ambiental.
SSD (Unidad de Estado Sólido)	Bajo a Medio	Borrado Criptográfico (NIST Purge)	Rápido, eficiente, permite la reutilización.	Vulnerable si no hay sobrescritura física adicional.
SSD (Unidad de Estado Sólido)	Alto	Destrucción Física certificada	Máxima seguridad, irrecuperable.	Inutiliza el dispositivo.
Medios Magnéticos (Cintas)	Todos los niveles	Desmagnetización	Rápido y eficiente para grandes volúmenes.	No aplica a SSD.
Medios Ópticos (CD/DVD)	Todos los niveles	Trituración o Incineración	Destrucción definitiva y segura.	Inutiliza el dispositivo, impacto ambiental.

En conclusión, el borrado digital seguro es un pilar fundamental en la protección de la información y la gobernanza de datos. Como se ha demostrado, la simple eliminación o el formateo no son suficientes para proteger los datos confidenciales, lo que expone a individuos y organizaciones a riesgos legales, económicos y de reputación inaceptables. Su implementación no es un acto técnico aislado, sino una estrategia de negocio crítica que debe integrarse en la política de seguridad de la información de toda entidad.

	<b>PLAN DE PRESERVACION DIGITAL</b>	<b>Código: ANL04</b>
		<b>Versión: 2</b>

La Institución es consciente de la evolución de las tecnologías y los estándares, reconociendo que un método fiable para un disco duro magnético puede ser ineficaz para una unidad de estado sólido moderna. La elección del método será un proceso de toma de decisiones informado, que considere no solo el nivel de seguridad requerido por la confidencialidad de los datos, sino también el tipo de medio de almacenamiento, el costo y el impacto ambiental.

La Institución adoptará un enfoque de defensa en profundidad, combinando métodos como el borrado criptográfico con la sobrescritura certificada para datos de alta sensibilidad. Además, es imperativo utilizar herramientas de software o hardware que ofrezcan reportes de borrado verificados, ya que esta documentación es la prueba legal del cumplimiento normativo. A medida que la tecnología de almacenamiento y la capacidad de recuperación de datos continúen evolucionando, la seguridad de la información será un campo en constante cambio, lo que exige una adaptación continua de las políticas y herramientas para proteger los activos digitales.

#### 4.4. Fase 4 Plan de Acción

##### 4.4.1. Definición de Acciones y Estrategias

En los anteriores cuadros, se incluyeron las actividades o acciones definidas para cada uno de los riesgos identificados, así como la dependencia responsable de la ejecución de cada una de ellas.

##### 4.4.2. Definición de recursos y cronograma de ejecución

A continuación, se presenta el cronograma de ejecución de las actividades asociadas al Plan de Preservación Digital a Largo Plazo definido por la Institución:

#	Estrategia	Responsable	2026	2027	2028	2029
<b>1.</b>	<b>Almacenamiento alternativo</b>					
1.1	Estudio de mercado	Informática Corporativa Dependencias involucradas				
1.2	Gestión presupuestal	Dependencias involucradas Informática Corporativa Dirección Financiera				
1.3	Adquisición de medio alternativo	Dependencias involucradas Informática Corporativa				
1.4	Automatizar copias de seguridad en la nube	Proveedor externo				
1.5	Automatizar copias de seguridad en medios locales	Informática Corporativa				
1.6	Realizar pruebas de restauración	Informática Corporativa Proveedor externo				
1.7	Documentar los procesos de respaldo y recuperación	Informática Corporativa Proveedor externo				



POLITÉCNICO COLOMBIANO  
JAIME ESCALA CADAVID

## PLAN DE PRESERVACION DIGITAL

Código: ANL04

Versión: 2

#	Estrategia	Responsable	2026	2027	2028	2029
<b>2</b>	<b>Formatos abiertos y estándares</b>					
2.1	Evaluar formatos de archivo utilizados y convertirlos a formatos abiertos si es necesario	Coordinación de archivo Apoyo Informática Corporativa				
2.2	Crear / Actualizar inventario de formatos de archivo y su estado de preservación	Coordinación de archivo				
2.3	Establecer / Actualizar políticas de selección de formatos para nuevos activos digitales.	Coordinación de archivo				
<b>3</b>	<b>Mantenimiento de Metadatos</b>					
3.1	Realizar diagnóstico de los metadatos para asegurarse de que sean precisos y completos.	Coordinación de archivo				
3.2	Implementar o actualizar los metadatos relevantes	Coordinación de archivo				
3.3	Capacitar al personal en la importancia de los metadatos y en su correcta aplicación.	Coordinación de archivo Informática Corporativa				
<b>4</b>	<b>Migración</b>					
4.1	Analizar estado actual de hardware/software que podría requerir ser actualizado	Informática Corporativa Dependencias involucradas				
4.2	Revisar disponibilidad presupuestal	Dependencias involucradas Informática Corporativa				
4.3	Adquirir artefacto	Informática Corporativa				
4.4	Realizar respaldos necesarios	Informática Corporativa				
4.5	Preparar nuevo ambiente	Informática Corporativa Proveedor				
4.6	Restaurar información	Informática Corporativa Proveedor				
4.7	Validar la integridad de los archivos antes y después de la migración	Informática Corporativa Proveedor				
4.8	Documentar proceso	Informática Corporativa Proveedor				
4.9	Poner en funcionamiento	Informática Corporativa				

#	Estrategia	Responsable	2026	2027	2028	2029
	nuevo ambiente	Proveedor				
4.10	Seguimiento nuevo Sistema	Informática Corporativa Proveedor Dependencias involucradas				
4.11	Apagado de Sistema anterior	Informática Corporativa Proveedor				
<b>5</b>	<b>Archivamiento de medios sociales</b>					
5.1	Identificar las plataformas y cuentas de medios sociales que contienen información relevante	Coordinación de archivo Oficina asesora de comunicaciones				
5.2	Establecer un proceso de captura y almacenamiento periódico de estos datos	Informática Corporativa Coordinación de archivo				
5.3	Implementar herramientas especializadas de archivamiento de medios sociales	Informática Corporativa Coordinación de archivo				
5.4	Definir / actualizar políticas internas de retención de datos para los archivos de medios sociales	Coordinación de archivo				
<b>6</b>	<b>Educación y capacitación</b>					
6.1	Programar capacitación	Coordinación de archivo Desarrollo laboral				
6.2	Ejecutar programa de capacitación	Coordinación de archivo				
6.3	Crear / actualizar materiales y guías	Coordinación de archivo Informática Corporativa				
<b>7</b>	<b>Seguimiento plan de preservación</b>					
7.1	Selección de herramienta para el seguimiento	Coordinación de archivo				
7.2	Realizar seguimientos anuales del sistema de preservación y de los activos digitales	Coordinación de archivo Informática Corporativa				
7.3	Identificar acciones de mejora	Coordinación de archivo Informática Corporativa				
7.3	Implementar acciones de mejora	Coordinación de archivo Informática Corporativa				
7.4	Documentar los hallazgos y crear plan de acción	Coordinación de archivo Informática Corporativa				

 POLITÉCNICO COLOMBIANO JAIME ISAZA CADAVID	<b>PLAN DE PRESERVACION DIGITAL</b>	<b>Código: ANL04</b>
		<b>Versión: 2</b>

#### 4.4.3. Implementación del Plan de Preservación Digital

Para la implementación del plan de preservación digital a largo plazo en el Politécnico Colombiano Jaime Isaza Cadavid, es crucial seguir una estrategia integral que abarca la planificación, la tecnología, las políticas y la capacitación del personal. A continuación, se detallan los pasos clave:

- **Realizar el Diagnóstico y Planificación Estratégica**

El primer paso es realizar un diagnóstico para entender el estado actual de los activos de información de la institución, el cual se realizó y se presenta al inicio de este documento. Las otras actividades a realizar son las siguientes:

**Inventario de activos:** Identificar y catalogar todos los documentos, bases de datos, grabaciones de clases, investigaciones, etc., que necesitan ser preservados. Se debe incluir información como el formato, el tamaño, la ubicación, el nivel de importancia y la frecuencia de acceso.

**Evaluación de riesgos:** Analizar los riesgos que amenazan la integridad de la información, como la obsolescencia tecnológica, la degradación de los medios de almacenamiento y la pérdida de metadatos.

**Definición de políticas:** Establecer políticas claras sobre qué se preservará, por cuánto tiempo y con qué nivel de acceso. Esto incluye definir los formatos de archivo para la preservación (ej. PDF/A, TIFF, etc.).

- **Selección e Implementación de la Tecnología**

La elección de una solución tecnológica robusta es fundamental para la preservación a largo plazo.

**Sistema de preservación digital (DPS):** Implementar un sistema diseñado específicamente para este fin. Ejemplos de sistemas incluyen Archivemática, un software de código abierto, o soluciones comerciales como Rosetta de Ex Libris. Estos sistemas manejan procesos como la ingesta, el almacenamiento, la gestión de metadatos y el acceso seguro.

**Almacenamiento:** Utilizar una estrategia de almacenamiento diversificada y geográficamente redundante. Esto incluye acciones tales como:

- ✓ **Almacenamiento en la nube:** Servicios como Google Cloud Storage es el servicio que seguro que esta usando en este momento la Institución para el almacenamiento a largo plazo.
- ✓ **Almacenamiento local:** La Institución realiza copias de seguridad en servidores propios para un acceso rápido y como respaldo.
- ✓ **Almacenamiento externo:** La Institución está evaluando la posibilidad de almacenar copias de seguridad en una ubicación física diferente para protegerse contra desastres locales.

- **Gestión y Flujos de Trabajo**

 <p>POLITÉCNICO COLOMBIANO JAIME ISAZA CADAVID</p>	<p><b>PLAN DE PRESERVACION DIGITAL</b></p>	<p><b>Código: ANL04</b></p>
		<p><b>Versión: 2</b></p>

Se están estableciendo los procesos claros y automatizados para la gestión de los activos digitales a lo largo del ciclo de vida, tales com:

- ✓ **Ingesta:** Implementar un proceso estandarizado para la transferencia de archivos al sistema de preservación, asegurando que se capturen todos los metadatos necesarios.
- ✓ **Metadatos:** Utilizar un estándar de metadatos reconocido, como PREMIS (Preservation Metadata: Implementation Strategies), para registrar la procedencia, los derechos de autor, el historial de cambios y la información técnica de cada archivo.
- ✓ **Monitoreo y migración:** El sistema debe ser capaz de monitorear la integridad de los archivos y alertar sobre posibles problemas. También debe incluir herramientas para la migración de formatos obsoletos a nuevos formatos, garantizando la legibilidad a largo plazo.
- **Capacitación y Sostenibilidad**

La sostenibilidad del plan depende de la formación del personal y de un compromiso institucional a largo plazo. Para ello se planea realizar las siguientes actividades:

- ✓ **Capacitación:** Educar al personal de la Oficina de Archivo y Correspondencia, así como al personal de la Oficina de Informática Corporativa sobre los principios y prácticas de la preservación digital.
- ✓ **Colaboración:** Establecer alianzas con otras instituciones académicas o consorcios de preservación digital para compartir conocimientos, recursos y responsabilidades.
- ✓ **Financiación:** Asegurar un presupuesto recurrente para la compra de software, el mantenimiento de la infraestructura de almacenamiento y la capacitación del personal.

De esta forma, el Politécnico Colombiano Jaime Isaza Cadavid puede consolidar el Plan de Preservación Digital a Largo Plazo que sea robusto y sostenible, protegiendo su patrimonio intelectual y cultural para las futuras generaciones.

## 5. MONITOREO DEL PLAN DE PRESERVACIÓN DIGITAL -PPD-

El monitoreo es una función fundamental en el Plan de Preservación Digital a Largo Plazo. No se trata de una tarea única, sino de un proceso continuo y sistemático para garantizar que los activos digitales se mantengan accesibles, auténticos, íntegros y utilizables a lo largo del tiempo. A continuación, se detallan los elementos clave para realizar el monitoreo del Plan de Preservación Digital a Largo Plazo:

### a) Monitoreo de la Integridad de los Archivos

Este es el pilar fundamental del monitoreo. Su objetivo es detectar cualquier cambio o corrupción en los archivos digitales. Se realiza a través de las siguientes actividades:

 <p>POLITÉCNICO COLOMBIANO JAIME ESCALA CADAVID</p>	<b>PLAN DE PRESERVACION DIGITAL</b>	<b>Código: ANL04</b>  <b>Versión: 2</b>
---	-------------------------------------	---

**Checksums o huellas digitales (Hashes):** Se genera una huella digital única para cada archivo (ej. MD5, SHA-256) en el momento de la ingesta. El sistema de preservación verifica periódicamente estas huellas. Si el checksum cambia, significa que el archivo ha sido alterado o dañado. Las herramientas de preservación digital, como Archivematica, realizan esta verificación de forma automática y alertan sobre cualquier discrepancia que se pueda presentar en los archivos.

**Auditorías de integridad de archivos (FIM - File Integrity Monitoring):** Los sistemas de FIM monitorean y registran cualquier modificación en los archivos, incluyendo cambios en su contenido, permisos de acceso o metadatos. Esto es crucial para identificar cambios no autorizados, ya sean accidentales o maliciosos.

#### **b) Monitoreo del Estado del Almacenamiento**

Otro punto fundamental del monitoreo es la supervisión de la infraestructura donde se almacenan los archivos digitales, lo cual se debe realizar a través de las siguientes actividades:

**Verificación de medios de almacenamiento:** Revisar periódicamente la salud de los discos duros, cintas magnéticas, o la capacidad de respuesta de los servicios de almacenamiento en la nube.

**Redundancia y copias de seguridad:** Asegurar que las copias de seguridad se realizan de manera correcta y en ubicaciones geográficamente distintas. El monitoreo debe verificar que las copias son fieles a los originales.

**Detección de obsolescencia:** Identificar si los medios de almacenamiento o la tecnología utilizada se están volviendo obsoletos. Por ejemplo, si se están utilizando CD-ROMs o cintas, se debe planificar su migración a tecnologías más actuales antes de que sea imposible acceder a los datos.

#### **c) Monitoreo de la Obsolescencia Tecnológica y de Formatos**

Los formatos de archivo y el software pueden quedar obsoletos, haciendo que los documentos sean ilegibles con el tiempo. El monitoreo de este aspecto implica las siguientes actividades:

**Detección de formatos de archivo:** Utilizar herramientas como PRONOM/DROID para identificar y caracterizar los formatos de los archivos. Estas herramientas ayudan a saber si un formato es de preservación (ej. PDF/A) o si es un formato propietario que podría volverse inaccesible en el futuro.

**Planificación de la migración:** Si se detecta un formato obsoleto o en riesgo, se debe planificar la migración a un formato de preservación. El monitoreo debe seguir el progreso de esta migración y asegurar que se preservan los metadatos y la autenticidad del archivo original durante el proceso.

#### **d) Monitoreo de las Políticas y Procedimientos**

El monitoreo no es solo tecnológico; también es organizacional, por lo tanto, se deben realizar las siguientes actividades:

**Auditorías internas y externas:** Realizar auditorías periódicas para asegurar que se están

 <p>POLITÉCNICO COLOMBIANO JAIME ESCALA CADAVID</p>	<p><b>PLAN DE PRESERVACION DIGITAL</b></p>	<p><b>Código: ANL04</b></p> <hr/> <p><b>Versión: 2</b></p>
---	--	--

cumpliendo las políticas de preservación digital. Normas como ISO 16363 (Auditoría y Certificación de Repositorios Digitales Confiables) o criterios como TRAC (Trustworthy Repositories Audit & Certification) proporcionan marcos para evaluar la confiabilidad de los repositorios digitales.

**Revisión de flujos de trabajo:** Verificar que los procesos de ingesta, descripción y acceso a los archivos digitales se están llevando a cabo según lo planeado. Esto incluye el monitoreo del personal para asegurar que se están siguiendo los procedimientos establecidos.

**Análisis de riesgos:** Revisar y actualizar el análisis de riesgos regularmente para identificar nuevas amenazas (ej. nuevos tipos de ataques cibernéticos, cambios en las normativas, etc.) y adaptar el plan de preservación.

Para concluir, el monitoreo del Plan de Preservación Digital a Largo Plazo es un ciclo continuo que abarca la integridad de los datos, el estado de la infraestructura, la vigencia de los formatos y el cumplimiento de las políticas. Se apoya en una combinación de herramientas automatizadas y auditorías manuales para garantizar que los activos digitales de la institución se mantengan seguros y accesibles para siempre.

 <p>POLITÉCNICO COLOMBIANO JAIME ESCALA CADAVID</p>	<p><b>PLAN DE PRESERVACION DIGITAL</b></p>	<p><b>Código: ANL04</b></p>
		<p><b>Versión: 2</b></p>

## REFERENCIAS BIBLIOGRÁFICAS

ARCHIVO GENERAL DE LA NACIÓN. Fundamentos de Preservación Digital a Largo Plazo. Recuperado el 29 de julio de 2014 de [https://www.archivogeneral.gov.co/sites/default/files/Estructura\\_Web/5\\_Consulte/Rcursos/Publicacionees/FundamentosPreservacionLargoPlazo.pdf](https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/5_Consulte/Rcursos/Publicacionees/FundamentosPreservacionLargoPlazo.pdf)

ARCHIVO GENERAL DE LA NACIÓN. Guía para la elaboración e implementación del Plan de Preservación Digital. Recuperado de [https://www.archivogeneral.gov.co/sites/default/files/Estructura\\_Web/5\\_Consulte/Rcursos/Publicacionees/2022/GuiaPlanPreservacionDigital.pdf](https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/5_Consulte/Rcursos/Publicacionees/2022/GuiaPlanPreservacionDigital.pdf) el 01 de agosto de 2024

ARCHIVO GENERAL DE LA NACIÓN. Publicaciones. [En línea] 14 de Noviembre de 2017. [Citado el: 31 de Octubre de 2024.] [https://www.archivogeneral.gov.co/sites/default/files/Estructura\\_Web/5\\_Consulte/Rcursos/Publicacionees/DocumentoOficialV1\\_GuiaDocumentoYExpedienteElectronico26\\_ENE\\_2018\\_v3.pdf](https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/5_Consulte/Rcursos/Publicacionees/DocumentoOficialV1_GuiaDocumentoYExpedienteElectronico26_ENE_2018_v3.pdf)

COLOMBIA. Congreso de La República. Ley 594 de 2000. Por medio de la cual se dicta la Ley General de Archivos, Bogotá D.C., 2012, 16 p.

COLOMBIA. Congreso de La República. Decreto 1080 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura. Recuperado de <https://normativa.archivogeneral.gov.co/decreto-1080-de-2015/> el 21 de julio de 2024

NATIONAL LIBRARY OF AUSTRALIA. PADI Preserving Access to Digital Information. [En línea] <https://webarchive.nla.gov.au/awa/20110824015945/http://pandora.nla.gov.au/pan/10691/20110824-1153/www.nla.gov.au/padi/topics/19.html>

SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA (SAF). CORTOLIMA. PROGRAMA DE GESTIÓN DOCUMENTAL (PGD) 2019-2021. [En línea] 2019. [https://cortolima.gov.co/sites/default/files/images/stories/centro\\_documentos/PGD\\_CORTOLIMA\\_2019\\_2021.pdf](https://cortolima.gov.co/sites/default/files/images/stories/centro_documentos/PGD_CORTOLIMA_2019_2021.pdf)