POLÍTICA DE PRESERVACIÓN DIGITAL

La política de preservación digital tiene como fin establecer los lineamientos específicos que permitan a la entidad asegurar la estabilidad física de los datos, la permanencia y el acceso de la información de los documentos digitales y la protección intelectual garantizando los principios de la preservación digital de integridad, equivalencia, economía, actualidad, cooperación y normalización.

En tal sentido estará articulada con el proceso de gestión del riesgo, la política de seguridad de la información y con los instrumentos archivísticos establecidos en el Decreto 1080 de 2015, de tal manera que se pueda instrumentalizar la preservación digital. La política de preservación digital apoyará la transparencia en la gestión administrativa, la rendición de cuentas y brindará las garantías para la salvaguarda de los derechos de los ciudadanos, adoptando buenas prácticas orientadas a la racionalización de trámites y recursos, contribuyendo de esta forma, al cumplimiento de los objetivos institucionales en materia archivística, de conservación documental, transparencia, acceso a la información y transformación digital, permitirá el diseño y adopción de un modelo lógico de preservación a partir del plan de preservación a largo plazo establecido por el Instituto de Salud de Bucaramanga, conforme a lo dispuesto en el Acuerdo 06 de 2014 del Archivo General de la nación y en el Decreto 1080 de 2015.

1. OBJETIVO

Establecer los lineamientos, estrategias, principios y acciones que permitan garantizar la autenticidad, integridad, confidencialidad, fiabilidad, disponibilidad y equivalencia funcional de los documentos electrónicos de archivo y su preservación digital a largo plazo.

2. ALCANCE

La Política de Preservación Digital a Largo Plazo se encuentra diseñada para ser implementada transversalmente en la estructura orgánica de la ESE-ISABU, articulada y en coordinación entre las dependencias y con el propósito de normalizar la gestión electrónica de documentos en la entidad.

La Política de Preservación Digital a Largo Plazo, aplica para todos los documentos electrónicos de archivo, tanto nativos digitales como digitalizados, para los cuales se haya determinado como disposición final “conservación total” según las Tablas de Retención y Valoración Documental.

3. RESPONSABLE

El Gerente de la ESE ISABU, los jefes de oficinas, los demás funcionarios públicos y/o contratistas que tengan bajo su control o custodia documentos electrónicos de archivo.

4. DEFINICIONES

Disponibilidad: Entendida en un documento electrónico, como la capacidad actual y futura de que tanto el documento como sus metadatos asociados puedan ser consultados, localizados, recuperados, presentados, interpretados, legibles, y por tanto estar en condiciones de uso.

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

Documento nativo electrónico: Documento que ha sido elaborado desde un principio en medios electrónicos y permanecen en estos durante todo su ciclo de vida.

Documento digitalizado: Documento en soporte físico como el papel que se convierte o escanea para su utilización en medios electrónicos.

Emulación: Recreación en sistemas computacionales actuales del entorno software y hardware para permitir la lectura de formatos obsoletos.

Expediente electrónico de archivo: Conjunto de documentos electrónicos correspondientes a un procedimiento administrativo cualquiera que sea el tipo de información que contengan.

Fiabilidad: Entendida como la capacidad de un documento para asegurar que su contenido es una representación completa, fidedigna y precisa de las operaciones, las actividades, los hechos que testimonia o se puede establecer, declarar o sostener el acto o hecho del que es relativo, determinando la competencia del autor y examinando tanto la completitud en la forma del documento como el nivel de control ejercido durante su proceso de producción.

Integridad: Entendida como la cualidad de un documento para estar completo y sin alteraciones, con la cual se asegura que el contenido y atributos están protegidos a lo largo del tiempo. Es uno de los componentes que conforman la confianza del documento.

Medio de almacenamiento: Es un hardware que se utiliza principalmente para almacenar datos.

Migración: Cambio a nuevos formatos/plataformas (hardware y software) o nuevos medios.

Normalización de formatos: Establecer un catálogo de formatos a utilizar en la Entidad para la preservación digital y normalizar la producción documental con formatos de archivo de preservación a largo plazo.

Obsolescencia: Devaluación de un artículo debida al progreso tecnológico, lo cual sucede usualmente cuando una nueva tecnología o un nuevo producto sustituyen a otro más antiguo, que no tiene por qué ser necesariamente disfuncional.

Refreshing: Actualización de software o medios.

5. DESARROLLO

5.1. PRINCIPOS LA POLITICA DE LA PRESERVACIÓN DIGITAL

PRINCIPIO	DESCRIPCIÓN	CONTEXTO INSTITUCIONAL
INTEGRIDAD	Asegurar que el contenido informativo, la estructura lógica y el contexto no se han modificado ni se ha afectado el grado de fiabilidad ni la autenticidad del documento original.	La ESE-ISABU proporciona los recursos necesarios para la aplicación de controles en busca de preservar la confidencialidad, integridad y disponibilidad de esta, con el fin de promover el uso adecuado por parte de los funcionarios y personal provisto por terceras partes que se encuentren autorizados y requieran de ella para la ejecución de sus actividades
EQUIVALENCIA	Aplicar procesos, procedimientos, métodos y técnicas de preservación viables, prácticos y apropiados para el contexto de los documentos, de tal modo que se asegure la sostenibilidad técnica y económica de la preservación digital	La entidad se encuentra en la fase de digitalización y cargue para la conformación del expediente electrónico en el sistema de gestión documental electrónico de archivos
ACTUALIDAD	Evolucionar al ritmo de la tecnología y utilizar los medios disponibles en el momento actual para garantizar la preservación de los documentos en el futuro. Esto significa que un sistema de preservación digital debería mantener la capacidad de evolucionar, de ajustarse a los cambios dimensionales y añadir nuevas prestaciones y servicios.	Aplicar con base en buenas prácticas mecanismos de verificación de integridad de la información con herramientas de cifrado.
COOPERACIÓN	Reutilizar y compartir soluciones ya existentes y desarrolladas de forma conjunta con otros archivos digitales,	El GED se encuentra en constante proceso de integración con los diferentes sistemas de

	especialmente las relacionadas con los procesos que pueden ser gestionados de forma centralizada.	información de la entidad para el manejo centralizado de información.
NORMALIZACIÓN	Generar lineamientos y herramientas basadas en normas, estándares y buenas prácticas, como apoyo a la gestión y preservación de los documentos digitales.	A través de la implementación de los procesos correspondencia y archivo y del Sistema Integrado de Conservación y el Programa de Gestión Documental PGD.

SELECCIÓN Y ADQUISICIÓN

La selección de las soluciones tecnológicas relacionadas con el software y el hardware estarán basadas en el modelo de requisitos para la implementación de un Sistema de Gestión de Documentos Electrónicos (SGDE) del Archivo General de la Nación. De igual manera se tomarán como referencia los módulos descritos en las normas Internacionales para la selección de medios de almacenamiento para la preservación a largo plazo[1],

ACCESO Y USO

Los derechos de acceso y uso de los documentos por parte administradores, la comunidad y usuarios en general, se encuentran establecidos en el manual de seguridad digital, las tablas de control de acceso, el registro de activos de información y el índice de información clasificada y reservada de la ESE-ISABU.

5.2. ARTICULACIÓN DE LA PRESERVACIÓN DIGITAL CON LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

La ejecución de las diferentes estrategias para preservar los documentos electrónicos requiere del cumplimiento de las políticas de seguridad, de manera que se garantice la seguridad de la información específicamente en las siguientes acciones:

- Ejecutar procesos para la toma de copias de seguridad
- Controlar el acceso no autorizado
- Verificar la fiabilidad del software y hardware
- Detectar y neutralizar el ataque de virus o hackers
- Prever contingencias
- Identificar personal responsable de acceder a la información por cada dependencia.
- Sensibilización de los usuarios sobre el uso apropiado de contraseñas.

Así mismo, clasificar la información generada en la ESE-ISABU, según los establecido en el Esquema de Clasificación, el Índice de Información Clasificada y Reservada, y los niveles de acceso definidos en la Ley 1712 de 2014 (Público, Reservado y Clasificado) y adoptados en las Tablas de Retención Documental para las series y/o subseries documentales. De acuerdo a la Norma ISO 27000, que establece el modelo de referencia a la definición e implementación de un sistema de seguridad de información. Esta norma establece las políticas para el análisis, la detección y la posible solución de riesgos de tipo informático en un determinado sistema de información y están ligadas al ámbito de la gestión de documentos con acciones cuyo enfoque de aplicación se centra en el presente y corto plazo.

Algunos controles deben implementarse en materia de seguridad de la información y están relacionadas con la preservación digital, lo cual se relacionan a continuación:

- Seguridad organizacional.
- Desarrollo y mantenimiento de sistemas

[1] ISO/TR 17797:2016 “Archivo electrónico. Selección de medios de almacenamiento digital para preservación a largo plazo”, los formatos de fichero de documento electrónico, UNE-ISO 19005-1:2008 “Gestión de documentos. Formato de fichero de documento electrónico para la conservación a largo plazo. Parte 1: Uso del PDF 1.4 (PDF/A-1), la transferencia de datos e información NTC- ISO 14721:2018 Sistemas de transferencia de información y datos espaciales. Sistema abierto de información de archivo (OAIS).

- Control de acceso
- Seguridad del Personal
- Clasificación y control de activos

Los jefes de cada área podrán delegar el personal que tenga acceso a la información digital, adoptando las medidas que correspondan en materia de seguridad.

INDICADORES DE LA POLÍTICA DE PRESERVACIÓN DIGITAL

No.	Nombre del Indicador	Fórmula	Seguimiento
1	Efectividad en la gestión y cumplimiento del plan de Preservación Digital.	Actividades del Plan de Preservación ejecutadas / Actividades del Plan de Preservación programadas* 100	Anual

6. REFERENCIAS

Ley 594 de 2000, Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones. 14 de julio de 2000. Fecha de Consulta 5 de junio de 2022. En: https://normativa.archivogeneral.gov.co/ley-594-de-2000/

Archivo General de la Nación. Glosario de Términos. Fecha de consulta 20 de junio de 2022. En: https://glosario.archivogeneral.gov.co/vocab/

GTC ISO TR 18492:2013 Preservación a largo plazo de la información basada en documentos electrónicos. Instituto Colombiano de Normas técnicas y certificación.

7. CONTROL DE CAMBIOS

CONTROL DE MODIFICACIONES			
Versión	**Fecha**	**Descripción de la Modificación**	**Realizada por**
1	28-11-2023	Emisión inicial del documento	Profesional en Gestión Documental