CAPÍTULO 6

LA PRESERVACIÓN DE DOCUMENTOS DIGITALES COMO ESTRATEGIA NACIONAL PARA GARANTIZAR LA TRANSPARENCIA Y LA MEMORIA

Data de submissão: 04/09/2024 *Data de aceite: 01/11/2024*

Ma. Gabriela Castillo Solano
M.Sc. Docente de la carrera de Archivística de la Universidad de Costa Rica, Costa Rica.

Raquel Umaña Alpízar
M.Sc. Docente de la carrera de Archivística de la Universidad de Costa Rica, Costa Rica.

PALABRAS CLAVE: Documentos digitales, preservación digital, política de preservación, estrategias de preservación digital.

La cuarta revolución industrial nos ha alcanzado, trayendo consigo innovaciones, retos y hasta nuevos paradigmas; donde los avances tecnológicos desempeñan un papel preponderante, en cuanto al acceso a la información, acortar distancias y tiempos. Para ello, las organizaciones están apostando al uso de la tecnología y con ella, de los documentos electrónicos para maximizar su eficacia y al mismo tiempo ser más eficientes.

En este panorama, lo inmaterial se está convirtiendo en la única evidencia de nuestro conocimiento y de nuestra huella como sociedad, lo que vuelve urgente la implementación de técnicas y métodos para asegurar la preservación de la memoria organizacional y colectiva, pero también para garantizar la evidencia de la legalidad y de la transparencia en la gestión de las organizaciones.

La norma ISO 13008:2012 define preservación como: “Los procesos y operaciones realizados para garantizar la permanencia intelectual y técnica de los documentos auténticos a lo largo del tiempo” (pág. 8); por lo que, la preservación digital debe asegurar el acceso a la información digital a largo plazo, manteniendo el valor de sus propiedades significativas, en un ambiente en constante evolución; razón por la cual los desafíos deben considerar la obsolescencia tecnológica.

Sumado a lo anterior, el conjunto de documentos en soporte digital crece en ausencia de regulaciones, dificultando la preservación de los documentos esenciales

para la administración y la toma de decisiones, es impostergable contar con una estrategia nacional que permita garantizar la autenticidad, perdurabilidad y acceso a los documentos digitales; uno de los desafíos más apremiantes de la época.

La preservación de la evidencia y la historia contenida en los documentos digitales fortalece la transparencia, la gestión administrativa en general, asegura a la ciudadanía gozar y mantener sus derechos. Desarrollar una política nacional y estrategias de preservación digital que aseguren el acceso a los documentos, garantizando a la vez su autenticidad e integridad a lo largo del tiempo, es un deber para con la patria, la ciudadanía y las nuevas generaciones.

OBJETIVOS

Objetivo General:

Incentivar la implementación de la preservación digital mediante el desarrollo de políticas y estrategias nacionales, que aseguren el acceso a los documentos y garanticen la evidencia de la legalidad y de la transparencia en la gestión institucional y la memoria organizacional y colectiva.

Objetivos Específicos:

1. Identificar los elementos mínimos requeridos para la preservación de los activos de información en entorno digital que son producto de las funciones de las organizaciones.

2. Proporcionar una guía para la elaboración de políticas y estrategias de preservación digital para la administración y conservación de documentos digitales auténticos, íntegros y confiables a través del tiempo.

METODOLOGÍA

Se basa en la metodología utilizada para el Trabajo Final de Investigación aplicada de la Maestría Profesional en Administración Universitaria de la Universidad de Costa Rica, denominado "*Modelo de Preservación de Documentos Digitales en la Administración Universitaria. Estudio de caso: Universidad Nacional"*; el cual se desarrolló con el objetivo de proponer un modelo aplicable que garantice la administración y la conservación de los documentos digitales que se producen en las organizaciones, así como su autenticidad, perdurabilidad y el acceso a la información contenida en esos documentos digitales a través del tiempo.

La investigación es cualitativa por lo que se llevó a cabo un análisis de modelos de requisitos internacionales para determinar las mejores prácticas aplicables al contexto en

que fue desarrollada. Asimismo, es una investigación aplicada que indica las estrategias para la preservación de documentos digitales, con el fin de enfrentar los retos de la obsolescencia tecnológica y la conservación a largo plazo de activos de información en soporte digital.

La revisión bibliográfica y documental es la técnica por medio de la que se recolecta información a través de libros, artículos, tesis, guías, folletos, entre otros; por lo tanto, para el desarrollo de la investigación se utilizaron fuentes bibliográficas y documentales primarias y secundarias, tales como: normas y modelos internacionales y legislación aplicable, artículos científicos sobre archivos digitales, bases de datos de texto completo, entre otros.

Respecto al tratamiento de la preservación digital se toma como referente la Norma ISO 14721: Sistemas de transferencia de datos e información espaciales. Sistema abierto de información de archivo (OAIS); así como la metodología utilizada por el profesor Jordi Serra Serra, Máster de Gestión Documental de la Universidad de Barcelona (MGDIE), en la asesoría y capacitaciones brindadas a la Universidad de Costa Rica[1], y la experiencia del proyecto ARCA[2].

ELEMENTOS REQUERIDOS PARA LA PRESERVACIÓN DIGITAL: GUÍA PARA LA ELABORACIÓN DE POLÍTICAS Y ESTRATEGIAS DE PRESERVACIÓN DIGITAL

1. Política de Preservación Digital[3]

La preservación no trata solo de almacenar, sino que fortalece la gestión organizacional; por tal razón, se debe establecer una política de preservación digital, que debe estar alineada y ser consecuente con las políticas nacionales y organizacionales existentes.

El primer elemento de esta guía es la Política de Preservación de Documentos Digitales, que tiene como propósito la conservación y el acceso a los documentos digitales producto de las funciones sustantivas de la organización, garantizando la integridad, autenticidad y confiabilidad de la información a través del tiempo.

En este sentido, las políticas de preservación se deben elaborar contemplando la ejecución de los siguientes aspectos:

a. Promover la adecuada gestión de los documentos que garantice información fidedigna, para la toma de decisiones, la eficiencia, la rendición de cuentas, la gestión de los riesgos y la preservación de la memoria organizacional.

b. Preservar los documentos de archivo que se producen en las organizaciones

1 Actividades organizadas por la Universidad de Costa Rica en 2012, 2013 y 2017.
2 Repositorio Digital de Preservación Digital utilizado en el Archivo Nacional de Costa Rica y desarrollado por la empresa *Business Integrator Systems* (www.bis.co.cr), de la cual se recibió asesoría durante el proceso de investigación.
3 La estructura o formato de las políticas de preservación digital puede variar dependiendo del contexto nacional y organizacional, así como de las disposiciones normativas existentes.

en soporte digital y que deben conservarse a través del tiempo, garantizando la autenticidad, integridad y acceso a los activos de información; así como la designación clara de los responsables de la preservación de los documentos.

c. Establecer los requisitos estratégicos, legales, técnicos, tecnológicos y funcionales, con el fin de asegurar la continuidad, conservación e integridad del Archivo Digital.

d. Desarrollar un esquema de metadatos para garantizar la conservación de la información de contexto y las propiedades significativas que permitan la continua accesibilidad, usabilidad, significación y valor probatorio de la información contenida en los objetos digitales, a través del tiempo y de los cambios tecnológicos.

e. Aplicar las estrategias de preservación necesarias y el aprovisionamiento de nuevos servicios para la preservación de la herencia en soporte digital, mediante el aprovechamiento de las tecnologías de la información y la comunicación; disponer de los medios y recursos requeridos para facilitar, preservar y garantizar el acceso a la información a través del tiempo.

2. Estrategias de Preservación[4]

Las estrategias de preservación, segundo elemento de esta guía, tienen como fin establecer una propuesta de requisitos para el desarrollo y puesta en marcha de un Archivo Digital; dicha propuesta tiene un alcance estratégico y operativo en el ámbito organizacional.

Las estrategias que se proponen están fundamentadas en el Modelo de referencia de Sistemas de Información Abierta, Modelo OAIS (Norma ISO 14721), como una verificación conceptual dentro de los principios de repositorios digitales confiables, definidos por estándares internacionales y mejores prácticas.

a. Aspectos administrativos

- Archivo Digital: es el responsable de la preservación y de garantizar el acceso, autenticidad e integridad de los documentos en soporte digital. El Archivo Digital (AD) deberá formar parte del sistema de archivos de la entidad y estará a cargo de la Unidad de Archivo[5] la cual será responsable de la gestión de los recursos económicos, tecnológicos y humanos para su adecuado funcionamiento.

Además, la Unidad de Tecnología[6] debe asumir la responsabilidad de la gestión y aseguramiento de la infraestructura y plataforma tecnológica, en cumplimiento de los requerimientos operativos de la Unidad de Archivo, las propuestas de mejora y la

4 El diseño de las estrategias de preservación digital está basado en el modelo PLATTER, DPE Repository Planning Checklist and Guidance. DPED 3.2 April 2008; en el Modelo OAIS, Norma UNE-ISO 14721: 2015 y en la asesoría realizada por Jordi Serra Serra en la Universidad de Costa Rica en el año 2013.

5 Entiéndase como la instancia de la organización responsable de la gestión de documentos y archivos; ya sea el Archivo Central, Archivo Institucional, Departamento de Archivo, Oficina de Archivo, Unidad de Gestión de Documentos, Dirección de Gestión Documental, etc.

6 Instancia de la organización responsable de las tecnologías de la información y la comunicación; según se denomine: dirección, unidad, oficina, departamento, etc.

actualización de los componentes tecnológicos involucrados.

- Comisión Institucional de Preservación Digital (CIPD): es el órgano rector a cargo de coordinar, emitir y actualizar las políticas, estrategias y lineamientos institucionales en cuanto a la preservación digital y al desarrollo del Archivo Digital. Entre las principales funciones de la CIPD se pueden citar: emitir las directrices y lineamientos que deben aplicarse en materia de preservación digital, establecer las estrategias necesarias para el adecuado funcionamiento del AD, proporcionar la guía para la utilización de los recursos presupuestarios, humanos, equipo y de los servicios e intervenir en la resolución de conflictos que involucren a los productores, usuarios y encargados del Archivo Digital.
- Recurso Humano: la organización deberá poner a disposición del AD el recurso humano necesario para su óptimo funcionamiento, además se debe procurar que el personal a cargo tenga la formación académica idónea y su constante actualización para cumplir con sus funciones a la altura de la evolución tecnológica; para ello se debe disponer de un programa anual de capacitaciones.

El colaborador responsable del AD será conocido como Senior Information Risk Owner (en adelante SIRO), será el funcionario encargado de administrar el AD y de aplicar las estrategias de preservación, debe tener la capacidad para dirigir, liderar, crear políticas y procedimientos que permitan la preservación y seguridad de la información.

- Presupuesto: la CIPD debe definir de forma anual los recursos necesarios para la aplicación de las estrategias de Preservación Digital, así como para el mantenimiento, actualización y crecimiento de la plataforma y de la infraestructura que la soporta, para efectos de almacenamiento, mantenimiento y actualización de la solución de AD y para el programa de capacitación.
- Requisitos para las transferencias entre sistemas: el repositorio del AD debe estar en condiciones para recibir documentos e información de los diferentes sistemas existentes en la organización, para lo cual debe existir aprobación de la Unidad de Archivo; estas transferencias deben realizarse de conformidad con lo establecido en un Protocolo de Transferencia, previamente pactado entre las partes.

Además, la Unidad de Tecnología, será la encargada de supervisar y autorizar los servicios, aplicaciones e integraciones para las transferencias y/o comunicación entre los sistemas, de acuerdo con las necesidades definidas por la CIPD, garantizando la interoperabilidad, autenticidad e integridad de los documentos electrónicos durante su traslado, migración y almacenaje.

b. Plan de Datos

La definición de las características de la información de contexto y la contenida en los documentos a preservar es responsabilidad de la Unidad de Archivo, y deberá ejecutarse de conformidad con las directrices del Comité Institucional de Selección y Eliminación de

Documentos (CISED)[7] y del CIPD. El intercambio y almacenamiento de información se debe gestionar de acuerdo con los siguientes tipos de paquetes/contenedores de información, según lo establecido en el modelo OAIS, a saber:

- **Paquete de Transferencia de Información (*SIP*):** se utiliza para la transferencia, el *Submissión Information Package* (*SIP*, por sus siglas en inglés) es la información de contenido y descripción de los documentos (procedencia, contexto, referencias, derechos de acceso, autenticidad, integridad, etc.) que se entrega por parte de las instancias organizacionales al AD, para usarla en la construcción del paquete de información de archivo o *AIP* (*Archival Information Package*).

El procesamiento del *SIP* se puede realizar de dos maneras: el método *pull*, que implica que el repositorio disponga de un agente "de intermediación" que "recoge" el material; o el método *push*, mediante el cual el *SIP* se entrega en el repositorio para su procesamiento por parte del sistema u organismo productor original. Indistintamente de la forma de ingreso, es esencial la verificación de la ausencia de *malware* y de la integridad del documento transferido, la validación de datos, generación de metadatos, extracción de las propiedades significativas y aseguramiento de la calidad del paquete.

- **Paquete de Información de Archivo (*AIP*):** es el que se conserva en los repositorios, el *Archival Information Packa*ge (*AIP*, por sus siglas en inglés) es el paquete en que se ejecutan los procesos de preservación y que contiene la información de contenido, descriptiva, de relaciones y la información de conservación asociada, incluidas las modificaciones necesarias para ser almacenado en el AD, así como el fichero mismo auto-contenido en la estructura del paquete.
- **Paquete de Consulta de Información (*DIP*):** se genera para consumo como producto de una consulta, el *Dissemination Information Package* (*DIP*, por sus siglas en inglés) es el paquete de información creado por el AD y derivado del *AIP*, para distribuir el contenido digital que es consultado por los usuarios o por los sistemas que tienen acceso al Archivo Digital.

El *DIP* se materializará en forma de fichero único, que tendrá la consideración de copia auténtica de los documentos custodiados en el AD; además, del índice de contenedor (firmado electrónicamente), con los metadatos de la unidad documental a la que corresponda cada fichero y con un resumen criptográfico; o mediante un hiperenlace a la ubicación relativa de cada fichero, o puede contenerse dentro del paquete en su forma de copia de consulta.

Los ficheros podrán facilitarse en un formato distinto del que se custodia en el *AIP* o podrán reproducirse en el momento de la consulta, sin que tenga que conservarse el documento en el formato para consulta; es necesario recalcar que debe ejecutarse de forma previa una evaluación de acceso, que permita establecer si un usuario determinado

7 Según el artículo 33 de la Ley No. 7202 del Sistema Nacional de Archivos de Costa Rica, el CISED es el órgano competente para evaluar y determinar la vigencia administrativa y legal de sus documentos de la organización.

puede consultar un documento específico.

c. Plan de Ingreso

Este plan establece los servicios y funciones para recibir el *SIP*, es el proceso de transferencias de aquellos documentos digitales que, como parte de una estrategia de preservación, pasen a formar parte del Archivo Digital.

El ingreso de documentos al AD se puede realizar por medio de transferencias automáticas o asistidas, pero siempre por los canales definidos, y se podrán realizar de forma regular en un plazo acordado, conforme a lo que determine el Protocolo de Transferencia, para lo cual debe especificarse el detalle y el método (*push* o *pull*), lo cual puede realizarse por Serie Documental[8] o por Sistema Institucional, con el fin de establecer la estructura, contenido y forma.

Para esta tarea se debe oficializar un documento en el que se consignen las condiciones y los requisitos para la transferencia de los documentos al AD, el cual será el *Protocolo de Transferencia*, mismo que se elabora en conjunto entre la instancia productora de los documentos y la Unidad de Archivo.

El protocolo de transferencia debe contener al menos la siguiente información: alcance, formas de transferencia, estructura del *SIP*, formatos de fichero admitidos, esquema de metadatos, mecanismos de control y validaciones, derechos para realizar acciones de preservación sobre los documentos, plazo de conservación, propiedades significativas coleccionables, derechos de uso y acceso, fecha de vigencia del protocolo.

d. Plan de Conservación

El plan de conservación proporciona los servicios y funciones de control del entorno del Archivo Digital e incluye las estrategias técnicas con el objetivo de mantener, a través del tiempo, las características de integridad, autenticidad y acceso a la información que se encuentra en custodia. Por lo tanto, en el plan de conservación se contemplan los siguientes aspectos:

- Almacenamiento**:** se requiere proveer los servicios y plataforma para el almacenamiento seguro, mantenimiento y recuperación de los *AIP*.
- Condiciones de conservación de los documentos: los documentos conservados por el AD deberán tener una representación tecnológica vigente, codificada en el formato actualizado establecido por el SIRO, y deberán mantener las relaciones estructurales propias de dichos documentos.
- Monitorización y detección del riesgo: se debe dar seguimiento a los cambios en los requisitos del servicio y a los cambios tecnológicos (amenazas, soportes, formatos, sistemas y plataformas informáticas), para identificar tendencias

8 Las series que se concreten en sistemas de información se considerarán recapitulativas.

tecnológicas emergentes que podrían ser motivo de riesgo u obsolescencia en el entorno tecnológico del Archivo Digital y que impidan, potencialmente, el acceso y la preservación en el tiempo de los documentos, así como de la información custodiada por el AD; dicha función de revisión periódica le corresponde al SIRO.

- Proceso de migración: las migraciones pueden implicar cambios en los objetos de datos de contenido y/o en la información de representación a nuevos formatos, por lo que puede implicar el desarrollo de nuevos *AIP*, planes de pruebas, implementación y revisiones para la ejecución automática de las transformaciones, con el fin de reducir las probabilidades de pérdida de información.

Este proceso por lo general es complejo y costoso, por lo que se debe realizar solamente en casos justificados, ya sea por deterioro del formato y/o soporte, porque se han identificado nuevos requisitos de los usuarios finales y/o para una mejor rentabilidad, debido a la evolución constante de la tecnología.

e. Plan de Acceso

En este plan se establecen los servicios de cara a las necesidades de los usuarios finales. El acceso a los documentos debe gestionarse usando procesos automatizados; para ello, es necesario determinar la existencia, descripción, localización y disponibilidad de la información almacenada en el AD. Por lo que, a las Unidades de Archivo les corresponde analizar el uso de los documentos e identificar los permisos de uso y acceso correspondientes.

El *permiso de uso* se refiere a la capacidad de establecer y autorizar una configuración de permisos y roles de los que dispone un usuario para realizar las distintas acciones que provee un sistema; debe realizarse en concordancia con las mejores prácticas expuestas en la ISO/IEC 27001 Sistemas de Gestión de la Seguridad de la Información. El *permiso de acceso* se refiere al componente de seguridad del Paquete de Información y Consulta.

Se debe desarrollar el conjunto de reglas que identifiquen derechos de acceso, así como el régimen de permisos y restricciones aplicables a los documentos, metadatos, expedientes y en general a todos los niveles de agrupación, siempre cumpliendo con la normativa institucional y nacional vigente. El AD debe tener la capacidad de brindar información para usuarios internos y externos a través de una interfaz de consulta, o mediante servicios de interoperabilidad para que consuman otras aplicaciones o sistemas.

f. Plan de Tecnología

- Infraestructura y Plataforma Tecnológica: la infraestructura del AD deberá ajustarse a las necesidades de almacenamiento, procesamiento, seguridad y comunicaciones y ser escalable y redundante, utilizando *software* y equipo con tecnología de vanguardia, pero confiable.

- Seguridad: la infraestructura del AD deberá garantizar la autenticidad, integridad y disponibilidad de los documentos, información y datos custodiados, cumpliendo con la normativa y los procedimientos establecidos en la organización para este fin. Asimismo, el Archivo Digital deberá contar con un programa de verificaciones de autenticidad e integridad, y de ensayos de los procesos de recuperación y continuidad de servicio; de dichas revisiones y pruebas se generarían informes de resultado, que se utilizan como insumo para gestionar la protección contra ataques informáticos y para la configuración de los procesos de recuperación en caso de desastres.
- Copias de seguridad: se deben mantener copias de seguridad incrementales en un soporte no alterable, realizadas con periodicidad diaria (las incrementales) y semanal para la copia base. Adicionalmente, debería existir un almacenamiento espejo en un sitio remoto donde estén resguardados los paquetes *AIP*, usando una tecnología distinta a la del sitio principal y que incluya mecanismos adicionales de seguridad para proteger la información.
- Pistas de auditoría: se debe contar con un registro histórico que permita identificar y rastrear todos los eventos o acciones realizadas en el AD, para detectar cambios no autorizados, problemas de autenticidad, registros de las operaciones de conversión y migraciones de los documentos; así como un comprobante de la destrucción de documentos.

g. Plan de Continuidad

Para garantizar la disponibilidad y la operación ininterrumpida del Archivo Digital se debe disponer de un "Plan de Continuidad" el cual será elaborado y actualizado por la Unidad de Tecnologías; con el propósito de estar preparados en caso de interrupciones del servicio causadas por factores internos o externos sin control (catástrofes naturales, eventos provocados por terceros, etc.) y con el fin de restablecer los servicios en un tiempo mínimo, en la mayor medida posible.

Como parte de la estrategia del AD se señala que, por la importancia de este servicio, el plan de continuidad debe contemplar ciertos componentes en referencia a los siguientes aspectos de la operación del Archivo Digital: continuidad del servicio, alta disponibilidad, continuidad financiera, continuidad del conocimiento y continuidad en caso de desastre; los cuales deben considerarse vitales para la continuidad del negocio de la organización.

CONCLUSIONES

Con la cuarta revolución industrial se hace necesaria la implementación de buenas prácticas, estándares, técnicas y métodos para garantizar la evidencia de la legalidad y de la transparencia en la gestión de las organizaciones; así como para asegurar la preservación de la memoria organizacional y colectiva. Por consiguiente, el desarrollo de políticas y

estrategias de preservación digital que aseguren el acceso a los documentos, garantizando a la vez su autenticidad e integridad a lo largo del tiempo, es un deber para con la patria, la ciudadanía y las nuevas generaciones.

La preservación digital representa uno de los desafíos impostergables que enfrenta la sociedad de la información, principalmente por la obsolescencia tecnológica, por lo que las organizaciones deben contar con una política y con estrategias de preservación que les permita aprovechar las tecnologías de la información y la comunicación, pero de una manera responsable, implementando un repositorio especializado en la preservación digital y una infraestructura tecnológica robusta que permita gestionar y administrar los activos de información en un entorno digital y que se garantice su acceso a través del tiempo.

Por lo tanto, se pretende incentivar la implementación de la preservación digital mediante el desarrollo de políticas y estrategias nacionales, que aseguren el acceso a los documentos y garanticen la evidencia y la memoria de las naciones; mediante la propuesta de una guía que oriente la elaboración de políticas y estrategias para la administración y conservación de documentos digitales auténticos, íntegros y confiables a través del tiempo.

REFERENCIAS

Asociación Española de Normalización y Certificación. (2013). *Norma UNE-ISO 13008:2013 Proceso de migración y conversión de documentos electrónicos. Información y documentación*. España: AENOR.

Asociación Española de Normalización y Certificación. (2015). Norma UNE-ISO 14721:2015 Sistemas de transferencia de datos e información espaciales. Sistema abierto de información de archivo (OAIS) Modelo de referencia. España: AENOR.

Castillo, M.G. y Umaña, R. (2018). *Modelo de Preservación de Documentos Digitales en la Administración Universitaria. Estudio de caso: Universidad Nacional.* (Trabajo final de investigación aplicada de Maestría Profesional en Administración Universitaria). Universidad de Costa Rica, Sede Rodrigo Facio.

Chaves, L. (2010). El paradigma cualitativo en la investigación educativa: una aproximación teórica. En Chaves, L., Díaz, M., García, J., Rojas, G., y Solís, N. (Ed.), *Investigación-Acción colaborativa: Un encuentro con el quehacer cotidiano del centro educativo para su transformación* (pp. 1-34). San José: INIE.

Ley N.° 7202 del Sistema Nacional de Archivos. La Gaceta: Diario Oficial de Costa Rica, San José, Costa Rica, 27 de noviembre de 1990.

Serra, J. (2014). Desarrollo de una Política de preservación digital como oportunidad de negocio para consultores y archiveros. Girona: Arxius i Indústries Culturals.

Serra, J. (2017). Taller de Preservación Digital para la Universidad de Costa Rica [Presentación]. San José.