REVISTA DEL ARCHIVO NACIONAL
RAN
2019 SAN JOSÉ, COSTA RICA AÑO 83

# Modelo para la preservación de documentos digitales[1]

## *Model for the Preservation of Digital Documents*

**María Gabriela Castillo Solano**

M.Sc. María Gabriela Castillo Solano, Docente de la Sección de Archivística de la Universidad de Costa Rica. mariagabriela.castillo@ucr.ac.cr | COSTA RICA.

**Raquel Umaña Alpízar**

M.Sc. Raquel Umaña Alpízar, Docente de la Sección de Archivística de la Universidad de Costa Rica. raquel.umana@ucr.ac.cr | COSTA RICA.

Fecha de recepción: 24/04/2019 | Fecha de aprobación: 21/11/2019
Sección de la RAN: Archivística

**RESUMEN.** Quizás la principal característica de la Era Digital es la rapidez de la evolución tecnológica, y con ella, la obsolescencia tecnológica como principal enemigo del acceso a la información. La preservación de documentos digitales, supone fortalecer la gestión administrativa debido a que los documentos son la base de la transparencia y el estado de derecho.

Se presenta un modelo de preservación digital que permita a las organizaciones garantizar autenticidad, perdurabilidad y acceso a los documentos a través del tiempo; contemplando

1 Trabajo ganador del premio "José Luis Coto Conde" de investigación archivística 2019.

un modelo de Archivo Digital, aplicable a la administración y conservación de los documentos digitales que se producen en las Instituciones de Educación Superior, pero también a cualquier organización pública o privada, para esgrimir el liderazgo implementando mejores prácticas y constituyéndose en casos de éxito.

**PALABRAS CLAVE.** Documento electrónico, gobierno electrónico, preservación digital, repositorio digital, tecnologías de la información.

**ABSTRACT.** *Perhaps the identifying aspect of the Digital Age is the fast development of technological evolution, and with it, the technological obsolescence's arrival as the main enemy of digital media information access continuity. Digital documents' preservation means strengthening administrative management, because documents are the basis of transparency and the rule of law.*

*We presented a digital preservation model that allows organizations to guarantee authenticity, durability and continuous access to the information contained on those documents over time; a comprehensive Digital Archive conservation and management model for those documents produced in Higher Eduction Institutions, but also applicable to any public or private organization, to take advantage of Higher Education Institutions' leadership in the embracement of best practices by becoming successful examples.*

**KEYWORDS.** *Electronic document, electronic governance, digital preservation, digital repository, information technologies.*

# 1. INTRODUCCIÓN

Durante el último siglo nuestra sociedad ha ido cambiado en muchos aspectos; dichas transformaciones traen consigo importantes retos y por consiguiente nuevos paradigmas por enfrentar. La suma de estas innovaciones conforma nuestra actualidad, que no se limita en la "sociedad de la información" sino que ha evolucionado a un punto donde se difumina el límite entre la humanidad y la tecnología.

El avance tecnológico ha permeado todas las áreas del quehacer humano, ya que permite un mayor acceso a la educación y a la información, se eliminan las barreras o limitaciones físicas y se aceleran los procesos, migrando hacia ese mundo virtual, lleno de objetos digitales, codificados y abstractos, de difícil compresión que se convierten en la única huella de nuestro paso por el tiempo y en la bóveda de nuestro conocimiento.

Las organizaciones, al igual que las personas, han ido migrando de un modelo basado en documentos en soporte papel a documentos electrónicos, buscando ofrecer un servicio más eficaz ante las necesidades de los usuarios y un uso más eficiente de los recursos que disponen; pero ese cambio supone también la necesidad de implementar procesos que permitan perpetuar esa huella de la vida institucional, no solo para la investigación y los propósitos científicos-culturales, sino para la garantía de la legalidad y la transparencia en la gestión organizativa; así como material de trabajo o consulta para las futuras generaciones que enfrentarán retos similares o que pueden beneficiarse de nuestra experiencia previa.

Por tanto, la preservación de los documentos digitales depende de una combinación de factores de *software y hardware*, ambos en evolución continua, por esto los desafíos son cada vez mayores a medida que el conjunto de documentos en formato digital crece y se vuelve obsoleto.

Este primer paso que se ha dado es solo eso, el primer paso en el mundo digital para una jornada que durará tanto como la humanidad misma, y que ya ha avanzado un amplio trecho en los otros soportes que se han usado para resguardar la información, información que define lo que somos, que cuenta quiénes fuimos y de dónde venimos, pero más importante aún, define hacia dónde nos dirigimos.

En este artículo se presenta una propuesta para enfrentar el reto de la continuidad del acceso a los documentos digitales, basada en los resultados obtenidos en 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*; desarrollado con el objetivo de proponer un modelo aplicable que administre y conserve los documentos digitales que se producen en las organizaciones y que permita garantizar la autenticidad, perdurabilidad y acceso a la información contenida en los documentos digitales a través del tiempo.

# 2. PROBLEMA Y JUSTIFICACIÓN

Las instituciones de educación superior y las organizaciones en general no escapan a la realidad de la evolución social que impone la incorporación de la tecnología a todos los campos de nuestro quehacer cotidiano ni a los riesgos que la incorporación de esas mejoras, producto de esa evolución, traen consigo debido al vertiginoso ritmo de avance tecnológico y los acelerados procesos de obsolescencia.

Conscientes de la necesidad de incorporar las nuevas tecnologías a fin de mantener la competitividad, las organizaciones automatizan procesos sin un análisis integral, generando de esta forma un riesgo que debe ser abordado, investigado y gestionado, a fin de garantizar la continuidad del ejercicio de sus funciones, la toma responsable de decisiones y la rendición de cuentas.

Al ser los documentos de archivo, el origen institucional de la información fidedigna, la base de la transparencia, y el elemento que habilita a la ciudadanía a reclamar y mantener sus derechos, es imperativo garantizar su acceso, integridad y autenticidad, en el presente y en el futuro.

El principal reto que generan los documentos digitales radica en el desconocimiento o desinterés del uso responsable de las TICs. Las organizaciones diseñan y utilizan sistemas informáticos, para gestionar sus funciones, pero como islas de información, sin dar garantía de la producción y conservación de documentos fidedignos, como lo concibe la *Norma ISO 15489:2016*.

Las instituciones adoptan sistemas digitales, muchas veces sin tener conciencia de los desafíos que plantea preservar a través del tiempo la integridad de la información contenida en los documentos y de la información que generan esos sistemas; o su valor administrativo-legal, o su eventual valor científico-cultural, ya que, no se trata solo de adquirir un certificado de firma digital para firmar documentos institucionales, o de digitalizar y almacenar información digital.

En consecuencia, la administración pública en general, y las universidades estatales en particular no disponen de una infraestructura para la preservación digital, ni de pautas organizacionales para la conservación de los documentos generados en este soporte.

La ausencia de planes institucionales para la implementación de repositorios de preservación digital, políticas o estrategias de preservación digital es una constante que se repite en la mayoría de las organizaciones públicas, de las que las instituciones de educación superior no son una excepción.

La gestión institucional de los documentos electrónicos, debe fundamentarse en el cumplimiento de mejores prácticas y estándares internacionales, aprovechando todo el conocimiento que ha permitido acumular el camino recorrido por instancias de otras latitudes, con el propósito de que la información contenida en los documentos digitales sea íntegra, accesibles, auténtica y utilizable a largo plazo; para ello las estrategias de preservación deben mitigar el efecto de obsolescencia, producto de la constante evolución tecnológica.

Las instituciones requieren contar con un plan estructurado para enfrentar los desafíos de la era digital, que permita preservar la información, uno de los pilares fundamentales de las entidades de educación superior.

La labor de la preservación digital es un proceso continuo de trabajo, que debe incluir ciclos de auto evaluación y transformación, de modo que permita enfrentar los retos futuros. Por tal razón, este trabajo de investigación pretende señalar los puntos claves que se deben considerar, especificando los requisitos básicos de preservación digital, que habiliten a las organizaciones para garantizar autenticidad, perdurabilidad y acceso a los documentos a través del tiempo; mediante la propuesta de un modelo que implementa las mejores prácticas archivísticas.

# 3. METODOLOGÍA

La investigación se fundamentó en el paradigma cualitativo, que según expresa Chaves (2010):

> (...) se preocupa por la comprensión de los fenómenos sociales mediante la captación e interpretación de los significados que las personas asignan a sus acciones, en su contexto, por lo que no busca la generalización de sus hallazgos. Su propósito es crear teoría para las condiciones y valores de la situación específica estudiada (p. 8).

Con la investigación cualitativa "se busca conocer con profundidad las necesidades, intereses y preocupaciones" (Krueger, 1988, citado por Ivankovich, 2011, p. 547). Al respecto, se puede decir que en la investigación se analizaron modelos de requisitos internacionales para determinar una propuesta que implemente las mejores prácticas de los modelos examinados, en el marco de la realidad nacional; aspectos determinantes en el establecimiento de una propuesta de Modelo de Preservación de documentos digitales.

Es una investigación descriptiva debido a que se detallan los requisitos administrativos, archivísticos y tecnológicos, los cuales son componentes necesarios para poner en práctica la propuesta. También es una investigación aplicada que propone un modelo de preservación de documentos digitales, para solucionar los problemas de obsolescencia tecnológica y su conservación a largo plazo.

Las técnicas de recolección de información son definidas por Solís (2007) como: "herramientas que permiten la construcción de los datos en un proceso de investigación" (p. 75); se hace referencia a que la recolección de datos implica la selección y aplicación de instrumentos de medición, con el fin de que las categorías en estudio y la información recabada puedan ser analizadas correctamente.

Específicamente la revisión bibliográfica y documental es la técnica por medio de la cual se recolecta información a través de libros, artículos, tesis, guías, folletos, entre otros; para el desarrollo de la investigación se utilizaron fuentes bibliográficas y documentales primarias y secundarias, a saber:

- Fuentes documentales primarias: normas y modelos internacionales y legislación nacional sobre el gobierno electrónico, documento electrónico, firma digital, sistemas de información y preservación digital.
- Fuentes bibliográficas primarias: artículos científicos sobre archivos digitales.
- Fuentes bibliográficas secundarias: bases de datos de texto completo como EBSCO del SIBDI, Dialnet, entre otros.
- Obras de referencia: diccionarios especializados.
- Recursos Electrónicos: Internet.

Además, en su momento se aplicaron entrevistas cualitativas; al respecto Solís (2007) manifiesta que: "es una técnica muy valiosa en la investigación cualitativa que permite identificar aspectos importantes y significativos de las personas informantes, desde su propia visión de mundo. Por lo tanto, profundiza en las creencias, pensamientos, valores y actitudes" (p. 78).

En dichas entrevistas se obtuvo información acerca de las categorías de análisis planteadas, con base en la entrevista estructurada y a partir de instrumentos especializados de aplicación en el ámbito internacional. Los instrumentos utilizados son los siguientes:

- Instrumento de Evaluación de Continuidad Digital y Gestión del Riesgo: cuestionario auto evaluable desarrollado por los Archivos Nacionales del Reino Unido (Risk Assessment Handbook. Kew: The National Archives, 2011).
- Cuestionario para la identificación del tipo de archivo digital: del modelo PLATTER del Digital Preservation Europe (DPE) (Repository Planing Checklist and Guidance DPED 3.2. April, 2008).

# 4. PRESERVACIÓN DIGITAL

Las organizaciones, al igual que las personas, han ido migrando al modelo basado en tecnología, buscando servicios más eficaces a las necesidades de los usuarios y un uso más eficiente de los recursos de los que se dispone; ese cambio supone también la necesidad de implementar procesos que permitan perpetuar la huella de la vida organizacional, no sólo para la investigación sino para garantizar el acceso a las evidencias y a la transparencia en la gestión organizativa, y como referencia para las futuras generaciones que enfrentarán retos similares y que podrán beneficiarse de estas experiencias.

En la actualidad, los países están llamados a asumir estrategias de gobierno que les permitan brindar servicios y poner a disposición la información producto del ejercicio de sus funciones, para la transparencia y la rendición de cuentas a los ciudadanos. Según lo estipulado en la Carta Iberoamericana de Gobierno Abierto, se debe procurar que los pilares, principios, mecanismos y estrategias que se exponen sean promovidos y potencialmente aplicados más allá de las fronteras del gobierno y la administración pública (Poder Ejecutivo), hacia

otros niveles, sectores de la sociedad, y poderes del Estado; para lo cual se requiere de un trabajo integral, transversal y complementario, con la finalidad de mejorar la calidad de los sistemas democráticos, el buen gobierno y la institucionalidad pública en su amplio sentido (2016, p. 16-17).

En Costa Rica, desde el 2005 con el establecimiento de la Ley N° 8454 de Certificados, firmas digitales y documentos electrónicos, se dotó de la legislación para agilizar los trámites públicos mediante el uso de las tecnologías de la información. Por lo tanto, las instituciones se han planteado la meta de migrar hacia el "cero papel", donde interesa utilizar el medio digital para que el proceso administrativo sea más fácil, más rápido, más barato e incluso más eficiente; pero ¿acaso nos interesamos por garantizar el acceso, la integridad y la autenticidad de los documentos electrónicos?

Las organizaciones están produciendo documentos electrónicos, sin consciencia de los riesgos que esto implica, al no contar con estructuras específicas y desarrolladas para su adecuada gestión y preservación. Además, en los procesos de desarrollo tecnológico y gestión del cambio no se dispone de procedimientos sobre preservación digital, no se toman en cuenta los efectos de la obsolescencia tecnológica, ni se articulan con mecanismos para garantizar la preservación de los documentos; razón por la cual la preservación de documentos digitales es un tema de debate internacional.

Muchas organizaciones almacenan su información en discos externos, dispositivos removibles, discos duro locales, servidores de correo y servicios en la nube; la transición del soporte papel al electrónico nos ha hecho pensar que preservar documentos digitales es sinónimo de repositorio y/o almacenamiento, por lo que algunas instituciones creen estar protegidas al tener un "repositorio institucional". Sin embargo, no han establecido pautas organizacionales para la conservación de los documentos electrónicos y deberían implementar un archivo digital basado en *software* específico de preservación soportado por un modelo de infraestructura adecuada y segura.

La preservación no es solamente rescatar y almacenar información digital, supone reposicionar y fortalecer la labor de los profesionales de la información para que cumplan un papel primordial, que permita una adecuada gestión y preservación de los archivos digitales en el tiempo; al ser los documentos de archivo la base de la transparencia y la

responsabilidad de las instituciones, es ese elemento el que permite a los usuarios reclamar y mantener sus derechos.

En razón de lo anterior, planteamos la siguiente interrogante: ¿qué tal sería leer este artículo o cualquier documento que hayamos elaborado hoy, en la computadora que utilizábamos en el año 2000?

Es poco probable, que un documento digital elaborado en el 2000 en un formato popular se pueda considerar confiable y seguro hoy, que se pueda adaptar al cambio de paradigma de las PC de escritorio de 16 bits, a los poderosos procesadores de múltiples núcleos de 64 bits que hoy residen hasta en nuestros dispositivos móviles; si esto se pone de manifiesto en tan sólo 19 años, qué podemos esperar para los documentos electrónicos que se generan hoy en nuestras instituciones, los cuales representan el valor probatorio de su operación no solamente desde el punto de vista de la transparencia o del valor histórico, sino desde el punto de vista de la gestión administrativa.

Por lo que, mantener los documentos digitales por tiempo indefinido, garantizando su autenticidad, integridad, confiabilidad, confidencialidad y disponibilidad de la información en todo momento, resulta todo un reto.

Una vez planteadas estas reflexiones, se mencionan algunos aspectos teóricos y conceptuales requeridos para comprender la propuesta de modelo de documentos digitales en Costa Rica.

La preservación está definida en la Norma ISO 13008 como: “Los procesos y operaciones realizados para garantizar la permanencia intelectual y técnica de los documentos auténticos a lo largo del tiempo” (p. 8). Ante esto, la preservación digital pretende asegurar el acceso a la información digital a largo plazo, manteniendo la capacidad de consultar y revisar el documento, sin importar su formato.

Al respecto Ferreras (2010) citando a J. Rothenberg (1995) menciona que:

> La preservación digital se define como un conjunto de procesos dirigidos a conservar la información en formato digital. No existe preservación digital si no se mantiene la posibilidad de acceder a los recursos digitales. El objetivo de la preservación digital es permitir a los futuros usuarios recuperar, acceder, descifrar, ver, interpretar, entender y experimentar documentos y datos de forma significativa y válida (p. 12).

A su vez, las Directrices para la Preservación Digital de la UNESCO (2003) definen la preservación como: las acciones destinadas a mantener la accesibilidad de los objetos digitales a largo plazo para hacer frente a peligros que pueden amenazar cualquiera de los elementos del objeto digital: material, lógico, conceptual y esencial, mediante la utilización de los principios: Patrimonio, Responsabilidad, Decidir qué conservar, Colaborar con los productores, Derechos, Control, Autenticidad y protección de los datos, Gestión y Trabajo en equipo (pp. 23-26).

En este sentido, el tema de la preservación es complejo, conlleva una serie de acciones y estrategias que se deben implementar a nivel institucional. Juan Voutssas (2011) menciona que:

> Los requerimientos para la preservación a largo plazo llevan al límite a las tecnologías actuales de información y administración de información. Preservar información digital a largo plazo requiere de sistemas, instituciones, modelos técnicos y de organización, personal calificado y experimentado lo suficientemente robustos para sortear fallos tecnológicos, cambios sucesivos de plataformas de cómputo, obsolescencia de medios y formatos de almacenamiento, errores humanos, negligencia y ataques malintencionados... (p. 14).

Uno de los elementos que afecta considerablemente la obsolescencia tecnológica son los formatos. La Norma ISO 13008 (2013) define *formato de fichero* como la codificación de un tipo de fichero que se puede representar o interpretar de una forma coherente, esperada y significativa, a través de la intervención de un determinado *software o hardware* que ha sido diseñado para administrar ese formato (p. 7).

Los tipos de formatos de preservación pueden variar de acuerdo con el uso que se le vaya a dar a la información contenida en el documento, pero deben utilizarse aquellos que tengan mayor inmunidad a la obsolescencia, tomando en cuenta la compatibilidad, popularidad, mantenimiento (actualizaciones), derechos de uso y respaldo.

Existen formatos específicos para cada tipo de objeto digital: gráficos, audio, videos, documentos, etc. Algunos formatos están asociados con una o más extensiones de archivo (cadena de caracteres anexados al final de un nombre de archivo separados por un punto) que los identifica. A continuación, se mencionan algunos formatos:

- Formatos para archivos de texto: DOC, DOCHTML, HTML, PDF, RTF, TXT.
- Formatos para imagen: GIF, BMP, JPE, JPEG, JPG, JPG2, PNG, TIF, TIFF.
- Formatos para archivos comprimidos: ZIP, RAR, ZOO, XXE, ACE, ARJ.

Cabe destacar que existen formatos que pierden o no información debido a procesos de optimización de tamaño; por ejemplo: los formatos JPEG, GIF y PNG eliminan la información del archivo por considerarla innecesaria (espacios en blanco o gamas de colores no visibles), sufriendo pérdida de información, pero no de calidad a efectos de visualización, con la ventaja de que requieren menos espacio de almacenamiento.

Como riesgo, se puede mencionar que los formatos, al depender de la tecnología, se desactualizan con el peligro potencial de pérdida de información; razón por la que los documentos se deben migrar a versiones actualizadas o a formatos vigentes, con el propósito de garantizar su disponibilidad.

De acuerdo con Brown (2008) los criterios para elegir los formatos de conservación a largo plazo son los siguientes:

- Estándares abiertos.
- Con presencia amplia en el mercado.
- Estables y con compatibilidad retroactiva.
- Con apoyo a la meta descripción.
- Con alta funcionalidad y baja complejidad.
- Interoperables.
- Robustos y con detección de errores.

Por su parte, Serra (2014) sostiene que es necesario caracterizar, identificar o reconocer de manera fiable el formato del documento, valorar el mantenimiento de las propiedades significativas por parte de dicho formato y transformar a un formato sobre el que se tenga más capacidad de control y confianza.

Otro aspecto fundamental para la preservación digital es el proceso de migración; la Norma UNE ISO 18492 la define como el "Proceso de transferir información electrónica basada en documentos de un entorno de *software*/*hardware* o soporte de almacenamiento a otro

entorno o soporte de almacenamiento con poca o ninguna alteración de su estructura, y sin alteración del contenido y contexto" (AENOR, 2016, p. 7).

De acuerdo con lo que establece el Modelo OAIS, se trata de una migración cuando se hacen cambios en los bits de la información de contenido con el fin de conservarlo:

> La Migración Digital se define como el traspaso de información digital, con el objetivo de conservarla al mismo tiempo, dentro del OAIS. Se distingue de las transferencias en general por tres atributos: se centra en la preservación de todo el contenido de la información que se pretende conservar; la perspectiva de que la nueva implementación de archivos de la información sustituye a la antigua; y el control y la responsabilidad totales de todos los aspectos del traspaso residen en el OAIS (Norma UNE-ISO 14721, p. 86).

Por su parte, a las migraciones digitales que requieren algunos cambios en la información de contenido se les llama *transformaciones*, estas modificaciones se aplican en algunos de los bits de la información de contenido (IDC) con los correspondientes cambios en la información de representación asociada (Norma UNE-ISO 14721, p. 91).

El Modelo OAIS identifica cuatro tipos de migración digital, que ordenados por riesgo creciente de pérdida de información son las operaciones que no modifican las secuencias de bits como el Refrescamiento/Recopiado y la Reproducción/Copia; y las operaciones que cambian las secuencias de bits como el Re-empaquetado y la Transformación (Norma UNE-ISO 14721, p. 89).

Adicional a la migración, también es necesario aplicar la conversión de los formatos de fichero; según Térmens (2013, p. 46): "los formatos de los ficheros pueden convertirse en obsoletos con el paso del tiempo, por lo que es necesario migrar los contenidos a un formato más actual para continuar teniendo acceso a los mismos".

La Norma UNE-ISO 13008 define *conversión* como el proceso de transformación de los documentos de un formato a otro, manteniendo las características del documento (p. 7). Por su parte, la *conversión de formato* es "La operación para convertir un documento digital a diferentes formatos electrónicos" (Norma UNE ISO 14641-1:2012, p. 9); se realiza para cambiar de estándar de codificación (formato del fichero) y obtener las ventajas de otro formato, con el fin de superar la obsolescencia tecnológica y procurando que sea un proceso reversible y sin pérdida de información.

Esto nos lleva al tema de las *Propiedades Significativas* ya que, ante las estrategias de conversión de los formatos de fichero, es necesario hacer un análisis de las propiedades significativas de los documentos, con el fin de conservar sus características. De acuerdo con el Proyecto INSPECT, las *"propiedades significativas"* son las características de los objetos digitales que deben ser conservadas a lo largo del tiempo para asegurar la continua accesibilidad, usabilidad y significación de dichos objetos (Recuperado de http://www.significantproperties.org.uk/).

Las propiedades significativas son las características de un objeto que deben mantenerse a través de las acciones de preservación; si un documento no conserva intactas sus propiedades significativas, se pueden ver afectadas condiciones como la calidad, disponibilidad y su representación visual. De acuerdo con lo indicado por Serra (2017), los tipos de propiedades significativas se citan a continuación:

- Contenido: expresión de la información, no necesariamente en una forma humanamente legible (texto, imágenes, etc.).
- Contexto: información que permite la comprensión del entorno tecnológico y administrativo con el que se relaciona, así como su procedencia.
- Apariencia: la forma en que el contenido del objeto se visualiza ante un agente o usuario (fuentes de letra, colores, etc.).
- Estructura: la organización de las partes que componen el objeto y cómo se relacionan unas con otras (cabeceras, paginación, etc.).
- Comportamiento: funcionalidades intrínsecas al objeto (enlaces hipertextuales, fechas actualizables, etc.)

Las propiedades significativas de un objeto digital están relacionadas con su contenido, contexto y estructura; Brown indica que los criterios para evaluar la equivalencia entre representaciones son:

- Autenticidad: conservar el contenido, la estructura y el contexto completos.
- Procesabilidad: conservar la capacidad de reutilizar la información (funcionalidades).
- Presentación: conservar la representación original como objeto conceptual (Brown, A. Digital Preservation Guidance 1. The National Archives, p. 3).

Por otro lado, Voutssás (2011) describe el Modelo de la Cadena de Preservación del Proyecto InterPARES e indica que es una secuencia de actividades y enfoques agrupados en varias etapas que conforman los "eslabones" de la cadena. De todas y cada una de estas actividades y elementos se han ido haciendo investigaciones y especificaciones detalladas, y su conocimiento profundo implica un estudio a fondo de ellas (p. 17).

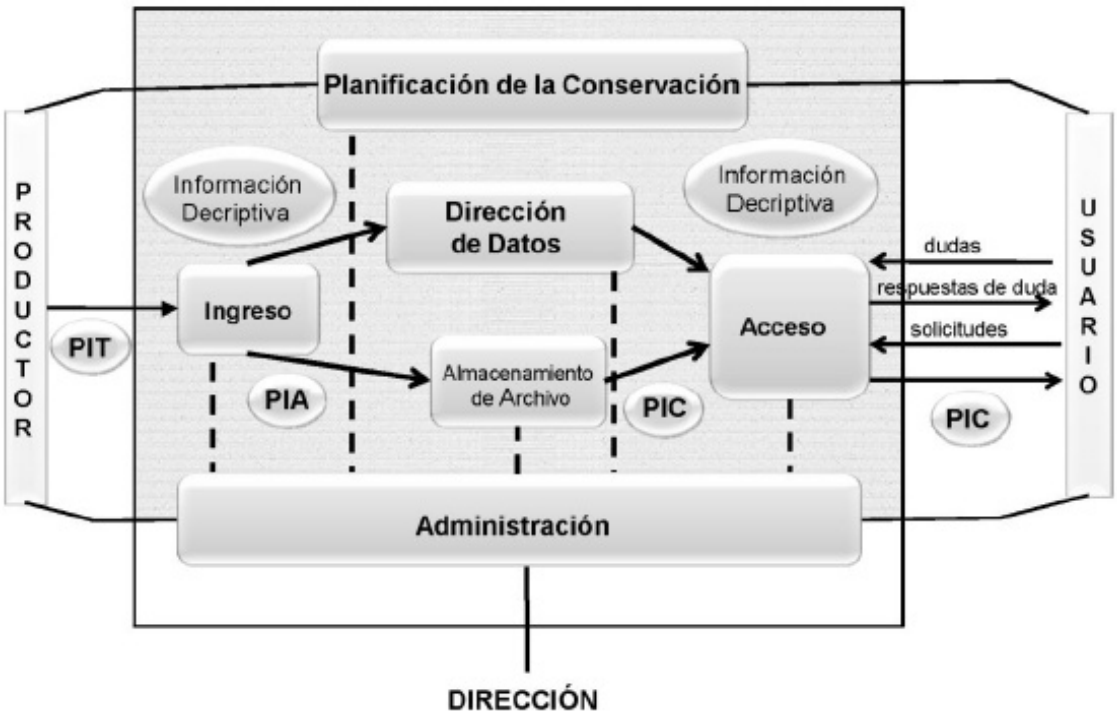
### 4.1. MODELO OAIS (OPEN ARCHIVE INFORMATION SYSTEM)

El Modelo OAIS es un marco de referencia que nace a finales del siglo XX en los Estados Unidos de América, como iniciativa de la National Aeronautics and Space Administration (NASA), para crear un sistema de transferencia de datos e información espacial que sirviera para identificar las características necesarias de un sistema de archivo. En el 2003, se transforma en la Norma ISO: 14721 Space Data and Information Transfer Systems (OAIS) siendo la iniciativa más completa y más adoptada por los grandes programas de preservación digital.

La Norma ISO 14721 estandariza la manera de gestionar los objetos digitales a través del tiempo, al tener en cuenta los cambios tecnológicos y previniendo su utilización fuera de su ambiente original; además, plantea el modelo conceptual para la creación de un Archivo OAIS, proporciona las características que debe tener un sistema de preservación de documentos digitales y ofrece el panorama de lo que se necesita para resguardar los documentos y asegurar el acceso de la información digital.

El Modelo OAIS se caracteriza por su entorno tridimensional compuesto por el productor de información, la dirección y el usuario; como eje central está el Archivo OAIS. Además, describe un modelo funcional, según se detalla a continuación:

**FIGURA 1. Entidades Funcionales de OAIS**




FUENTE: Norma ISO 14721:2015, p. 41.

- Ingreso: se preparan los documentos para la ingesta en el repositorio, aplicando controles que permitan el ingreso, control de procedencia, antivirus y formatos.
- Almacenamiento: se encarga del almacenaje físico de los documentos e incluye las estrategias de preservación fijadas, para garantizar el acceso de la información través del tiempo.
- Dirección de datos: en esta fase se conservan los metadatos que poseen los documentos, los que se generan en el proceso de la ingesta y los que se van incorporando durante la vida del documento.
- Preservación: se establecen las políticas y los responsables de vigilar los cambios constantes de la tecnología (revisión de formatos, *hardware*, *software*).
- Acceso: permite la accesibilidad al repositorio digital y a la consulta de los documentos por parte de los usuarios.

- Administración: es la integración de las funciones, los sujetos y la tecnología que interviene en el modelo OAIS.

En la Norma ISO 14721 se establecen los siguientes paquetes de información: Paquete de Información de Transferencia (*SIP*), Paquete de Información de Archivo (*AIP*) y Paquete de Información de Consulta (*DIP*) (AENOR, 2015, pág. 25). Además, se constituyen las responsabilidades que una organización debe cumplir para operar un Archivo OAIS, a saber:

- Negociar y aceptar la información adecuada de los productores de información.
- Obtener un control suficiente para garantizar la Conservación a Largo Plazo de la información proporcionada.
- Determinar la comunidad de usuarios del archivo, definiendo así su Base de Conocimiento.
- Asegurarse que la información a conservar es comprensible independientemente por la Comunidad de usuarios específica. En particular, ser capaz de comprender la información sin necesidad de recursos especiales como la asistencia de expertos.
- Seguir las políticas y procedimientos documentados que aseguran que la información se conserva contra todas las contingencias razonables, incluyendo la desaparición del Archivo, asegurando que nunca se elimine a no ser que sea permitido como parte de una estrategia aprobada.
- Hacer que la información conservada esté disponible para la Comunidad de usuarios, y permitir que la información sea consultada como copia, o como trazabilidad, de los Objetos de Datos originales transferidos, con evidencias que apoyan su autenticidad. (p. 37).

## 4.2. REPOSITORIOS DIGITALES

Para el almacenamiento de documentos en soporte digital se debe planificar la manera correcta de hacerlo; una de las acciones más importantes es contar con un repositorio de preservación digital. El Glosario de Preservación Archivística Digital define *repositorio institucional* como el "Conjunto de servicios e instalaciones ofrecidos por una organización a los miembros de su comunidad para el manejo y diseminación de materiales digitales producidos por la organización y sus miembros" (Voutssas, J. y Barnard, A., 2014, p. 189).

Para tener un repositorio de preservación digital la organización debe aplicar políticas y estrategias de preservación, de acceso, de metadatos y protocolos de transferencia, con el fin de garantizar que los documentos, y la información, este disponible en el presente y para futuras generaciones. Asimismo, el repositorio se debe encargar de recibir los documentos de otros sistemas institucionales, por medio de los protocolos de transferencia previamente establecidos.

La Norma UNE-ISO 17068 (2013) indica que un sistema de repositorio de documentos electrónicos debería estar equipado con las siguientes funcionalidades:

- captura, navegación y búsqueda de documentos electrónicos;
- emisión de certificados y documentos electrónicos;
- migración y recepción de documentos electrónicos;
- conversión de documentos electrónicos;
- comprobación de la integridad de los documentos electrónicos; y
- cierre y disposición de los documentos electrónicos (p. 24).

Por su parte, la Norma UNE-ISO 16363 (2017) refiriéndose a las auditorías y a los repositorios digitales de confianza, indica que en los repositorios se requiere una monitorización constante, planificación y mantenimiento, así como la implementación de estrategias y acciones conscientes para llevar a cabo su misión de conservación digital (p. 25).

### 4.3. ARCHIVO DIGITAL/ ELECTRÓNICO

La Norma UNE-ISO 14641 define archivo electrónico como el conjunto de acciones con el objetivo de identificar, capturar, clasificar, preservar, recuperar, visualizar y proporcionar acceso a los documentos con propósitos informativos, históricos o de conservación, requeridos para cumplir las obligaciones legales (AENOR, 2015, p. 9).

Para establecer la relación y la diferencia entre un sistema de gestión de documentos electrónicos de archivo o SGDEA (Electronic document and records management system o EDRMS por sus siglas en inglés) y un Archivo Digital (entendido en OAIS como el sistema de información archivística: Archival Information System) podemos señalar la intrínseca relación entre sus propósitos, más allá del objeto de trabajo que resulta común.

Un SGDEA es un sistema que captura, gestiona y provee acceso a los documentos; su principal objetivo consiste en llevar a cabo el proceso archivístico desde la creación de un documento, con funcionalidades como la homologación de la apariencia y características para tipos documentales a través del empleo de plantillas predefinidas, así como el control del flujo de trabajo de un determinado proceso, la descripción y la clasificación de documentos.

De acuerdo con la Norma ISO 15489 (2016) los sistemas de gestión de documentos comprenden una serie de elementos combinados, de manera que satisfagan los requisitos de gestión de documentos; por consiguiente, las aplicaciones de gestión documental deberían: aplicar los instrumentos de gestión de documentos; llevar a cabo procesos para crear, capturar y gestionar los documentos; y sustentar la creación y mantenimiento de relaciones lógicas entre el contenido de los documentos y los metadatos para la gestión de documentos (p. 12).

Un Archivo Digital consiste en la suma del repositorio digital como tal y la conjunción de personas y sistemas que han aceptado la responsabilidad de preservar la información y hacerla disponible a través del tiempo para una determinada población (ISO 14721, p. 4).

Por lo tanto, existe una evidente relación entre las funciones de ambos; sin embargo, es necesario aclarar que cuando el SGDEA asume el reto de la gestión del documento y el acceso a través del tiempo, está delimitando ese tiempo hasta que se cumpla el plazo de conservación, y se debe tomar una acción determinada para la disposición final (eliminación o transferencia del documento); mientras que el Archivo Digital apunta a la gestión y garantía de acceso por un largo plazo, que puede extenderse de forma indefinida.

El Archivo Digital hace uso de estrategias, técnicas y estándares con la finalidad de garantizar las mejores posibilidades de conservar el acceso a la información de un documento electrónico, dando fe de su integridad, autenticidad y de su información contextual o metadatos, gestionando el riesgo de la obsolescencia tecnológica que es inherente al continuo proceso de la evolución de la informática y la tecnología.

El cambio tecnológico es una amenaza real, por lo que dentro de los períodos de conservación documental debidos al valor primario (administrativo/legal), es factible que un documento tenga problemas derivados de la obsolescencia tecnológica, por lo que diseñadores de SGDEA han optado por incluir interfaces que faciliten la transferencia de contenidos entre

el SGDEA y las aplicaciones de preservación digital implementadas en su entorno (Pauline, 2008, p. 22); con el fin de mejorar las posibilidades de acceder a los activos de información a través del tiempo.

Una de las diferencias más importantes del Archivo Digital con respecto al SGDEA es el uso de los Paquetes de Información Archivística, como contenedores de toda la información de contexto, descripción y preservación; así como el documento y sus posteriores formatos renovados, elaborado utilizando una tecnología sin dependencia de determinado fabricante y asegurable a través de mecanismos criptográficos de firma digital y sellado de tiempo; lo cual, sumado a la ejecución de estrategias y políticas diseñadas con el propósito especializado de garantizar el acceso a la información a través del tiempo, supone un importante cambio de enfoque con respecto a las prioridades del SGDEA.

Por su naturaleza, el Archivo Digital tiene la capacidad de recibir documentos de múltiples fuentes, organizándolos según el cuadro de clasificación institucional y habilita a la institución para poner al alcance de sus miembros la información y el conocimiento organizacional, según la clasificación de acceso.

Un Archivo Digital es la evolución natural de la gestión de los documentos electrónicos realizada en los SGDEA, tal como el Archivo Central es la evolución de la gestión de los documentos en los Archivos de Gestión.

## 5. METADATOS

El metadato se define como: “la información que caracteriza o describe a otro recurso de información, especialmente con propósito de documentar, describir, preservar o administrar ese recurso” (Voutssas & Barnard 2014, p. 91); existen metadatos técnicos, tecnológicos, administrativos y de preservación.

Los metadatos se incluyen desde el momento en el que se crea un documento, pueden ser insertados manual o automáticamente y se van acumulando durante los eventos en la vida del documento, son parte integral de la información en custodia y deben ser protegidos de la

eliminación no autorizada. Según la Norma UNE-ISO 15489, los metadatos deberían consistir en información acerca de lo siguiente:

> a) una descripción del contenido del documento; b) la estructura del documento (por ejemplo su forma, formato y las relaciones entre los componentes que conforman el documento); c) el contexto de la organización, en el cuál el documento ha sido creado o recibido y usado; d) las relaciones con otros documentos y con otros metadatos; e) identificadores y otra información necesaria para recuperar y presentar el documento, como el formato o la información de almacenamiento; f) las acciones y operaciones de la organización sobre el documento a lo largo de su existencia (incluyendo la fecha y la hora de las acciones, cambios en los metadatos y los agentes que realizan estas acciones). Y afirma que ´los documentos que no poseen esos metadatos carecen de las características de un documento fidedigno. (AENOR, 2016, p. 12).

En la norma ISO 23081 sobre metadatos para la gestión de documentos, se incluyen principios, aspectos conceptuales y de implementación, y en la tercera parte se propone un método de autoevaluación del marco de gestión de metadatos. Asimismo, la Norma UNE-ISO 15489 indica que:

> Los metadatos se deberían definir para:
>
> **a.** permitir la identificación y recuperación de documentos;
> **b.** asociar los documentos con las cambiantes reglas de negocio, políticas y regulaciones;
> **c.** asociar documentos con agentes, y sus permisos y derechos sobre los documentos;
> **d.** asociar documentos con las actividades de la organización;
> **e.** y dejar huella de los procesos llevados a cabo sobre los documentos, tales como cambios en las reglas de acceso o migraciones a nuevas aplicaciones (AENOR, 2016, p. 21).

Además, plantea que los metadatos para la gestión de documentos deberían representar:

> **a.** el contexto de la organización;
> **b.** las dependencias y las relaciones entre los documentos y las aplicaciones de gestión documental;
> **c.** las relaciones con el contexto legal y social;
> **d.** las relaciones con los agentes que crean, gestionan y usan los documentos (*Ibid*, p. 11).

Según la Norma UNE-ISO 15489 "los metadatos de gestión de documentos se deberían describir y documentar en esquemas de metadatos. El desarrollo de los esquemas de metadatos se debería basar en los resultados de la identificación y valoración para el área o áreas de la organización que los va a aplicar" (*Ibid*, p. 12).

También, establece que "Los esquemas de metadatos se deberían desarrollar para definir qué metadatos se usan para identificar, describir y gestionar procesos de gestión de documentos. Para que los documentos tengan características de documentos fidedignos, los metadatos que tengan asociados deberían basarse en un esquema de metadatos autorizado." (*Ibid*, p. 20). Estos esquemas pueden relacionarse con diferentes entidades; las entidades clave para gestionar se citan a continuación:

**a.** Documentos: incluyendo todos los niveles de agrupación.
**b.** Agentes: incluyendo personas, unidades de negocio, tecnologías o aplicaciones de gestión documental y corporativa.
**c.** Actividades de la organización: funciones de negocio, actividades y operaciones o procesos de trabajo.
**d.** Regulaciones: leyes u otros requisitos que regulan las actividades de la organización y la creación o gestión de los documentos.
**e.** Relaciones: entre entidades y niveles de agrupación (*Ibid*, pp. 20-21).

### 5.1. PREMIS

PREMIS son las siglas de "Preservation Metadata: Implementation Strategies[2]" que es el nombre de un grupo de trabajo internacional patrocinado por Online Computer Library Center Incorporated (OCLC) y Research Libraries Group (RLG), quienes elaboraron un informe denominado PREMIS Data Dictionary for Preservation Metadata[3] (2010) que incluye un registro y definición de datos e información sobre los metadatos de preservación.

El diccionario de datos PREMIS (2008) define los metadatos de preservación como "la información que utiliza un repositorio para soportar el proceso de preservación digital" (p. 213). Además, se define un conjunto de unidades semánticas que utilizan los repositorios para

2 Metadatos de preservación: estrategias de implementación.

3 Diccionario de datos PREMIS de metadatos de preservación.

garantizar la perdurabilidad de los documentos, que sean recuperables y que evidencien los metadatos que se suman en el tiempo, así como las políticas del repositorio que almacena tales documentos.

Los metadatos de PREMIS se dividen en función de las siguientes entidades (p. 3):

- Entidad Intelectual: representación del objeto digital (documento, expediente).
- Objetos digitales: son unidades de información digital en sus diferentes presentaciones (ficheros, cadenas de bits o representaciones).
- Evento: acontecimientos/acciones que afectan a los objetos digitales.
- Agente: personas, organizaciones o *software*.
- Derechos: derechos y permisos.

### 5.2. METS

METS (Metadata Encoding & Transmission Standard), es un estándar de codificación y trasmisión de metadatos, propuesto por la Digital Library Federation con la finalidad de dotar un esquema de metadatos con la estructura de etiquetas XML, para describir y gestionar objetos digitales y permitir el intercambio de esos objetos entre repositorios.

La estructura METS consta de siete secciones principales las cuales se mencionan a continuación:

- Cabecera METS (Header): <mets:metsHdr>
- Metadatos descriptivos: <mets:dmdSec ID=”ID”>
- Metadatos administrativos: <mets:amdSec ID=”ID”>
- Sección Archivo: <mets:fileSec>
- Mapa estructural:<mets:structMap>
- Enlaces estructurales: <mets:structLink>
- Comportamientos: <mets:behaviorSec>

# 6. ANÁLISIS DEL CONTEXTO ORGANIZACIONAL Y EVALUACIÓN DE RIESGOS

En el marco de la implementación de un modelo de preservación de documentos digitales, de manera preliminar se debe realizar un análisis del contexto organizacional, con la finalidad de diagnosticar la situación en relación con la administración y conservación de sus documentos digitales, así como la evaluación de riesgos sobre la utilización y acceso de los objetos digitales que producen y reciben las organizaciones.

A continuación, se enlistan los aspectos que se deben analizar como parte del estudio de la situación actual de la organización:

- Escenario normativo: identificación y revisión del contexto normativo que regula el accionar de la institución y el cual permita la implementación del modelo de preservación.
- Escenario administrativo: se contextualiza acerca de las instancias que podrían asumir la responsabilidad del desarrollo y ejecución del modelo de preservación de documentos digitales.
- Escenario archivístico: se hace referencia a la gestión de documentos y archivos en la organización y al funcionamiento del sistema archivístico; así como a los procesos archivísticos que se ejecutan, los servicios y productos que se ofrecen, los recursos de los que disponen, entre otros.
- Escenario tecnológico: en este punto se contextualiza sobre los aspectos que garantizan la aplicación eficaz y eficiente de las TIC en la organización, acerca de la gestión y control de las tecnologías, la infraestructura tecnológica, la gestión de la seguridad, etc.
- Proyectos organizacionales: se identifican y describen los principales proyectos vinculados con la utilización de documentos digitales, desarrollados en la organización; como, por ejemplo: digitalización de documentos, migración de formatos, uso de la firma digital, sistemas de gestión de documentos electrónicos, entre otros.

Mediante el análisis del escenario normativo, administrativo, archivístico, tecnológico y de los proyectos que se han desarrollado, se puede determinar si la organización dispone de los elementos requeridos para la implementación de un proyecto de preservación digital; o si, por el contrario, se debe dotar de estos.

Además, permite identificar los aspectos funcionales y técnicos que la organización requiere para el establecimiento de un Archivo Digital, donde se asegure la conservación de los objetos digitales a través del tiempo.

Como parte del procedimiento a seguir, se realiza una evaluación del nivel de riesgo que afecta a los datos, documentos, sistemas y todo tipo de evidencias en formato electrónico que recibe o genera la organización. Para lo cual, se aplica el instrumento denominado "Digital continuity self-assessment tool", que es un cuestionario específico de autoevaluación desarrollado y utilizado por los Archivos Nacionales del Reino Unido, en el marco del *Digital Continuity Project*.

El informe de resultados sobre la evaluación de riesgos se presenta con el propósito de comprender el contexto organizacional y para identificar las acciones por implementar o que están en proceso de ejecución en la organización en materia de preservación digital.

El informe consta del análisis acerca de la evaluación de riesgos para la continuidad digital en la organización, en el cual se contempla lo siguiente: la continuidad digital como reto institucional e identificación de responsabilidades, la identificación de los requerimientos de información y dependencias tecnológicas, y la gestión de la información.

Finalmente, como parte del análisis de la situación se requiere evaluar el contexto con respecto al desarrollo de archivo digital para la organización en estudio; para ello, se aplica el cuestionario para la Identificación del Tipo de Archivo (modelo PLATTER del *Digital Preservation Europe*) y se presentan los resultados o conclusiones al respecto, los cuales versan sobre los siguientes elementos:

- Propósito y funciones del Archivo Digital.
- Dimensiones que debería tener el Archivo Digital.
- Operaciones diarias que se requieren regular para el Archivo Digital.
- Soluciones tecnológicas y aspectos sobre el proceso de implementación.

# 7. MODELO DE PRESERVACIÓN DE DOCUMENTOS DIGITALES[4]

El Modelo de Preservación de Documentos Digitales pretende proporcionar una solución metodológica para el desarrollo e implementación de un Archivo Digital, que permita garantizar el acceso, autenticidad, integridad y fiabilidad a la información archivística, como parte de una gestión de calidad en las instituciones públicas, facilitando nuevos servicios y la preservación de la herencia en soporte digital.

Comprende iniciativas y soluciones en diferentes áreas, desde el campo administrativo de alto nivel hasta herramientas específicas para obtener un fin, a continuación, se detallarán las más importantes.

## 7.1. ESTRATEGIAS DE PRESERVACIÓN

Las estrategias de preservación deben tomar en cuenta los requisitos estratégicos, legales, técnicos, tecnológicos, funcionales y las necesidades de los usuarios, para el desarrollo y puesta en marcha de un Archivo Digital, considerando el alcance estratégico y operativo a nivel institucional. A nivel Nacional en Costa Rica, la definición de las Estrategias de Preservación debe estar a cargo de la Dirección General del Archivo Nacional.

### 7.1.1. Política de Preservación Digital

Como parte de las estrategias de preservación, se debe establecer una política de preservación digital, que tenga como propósito conservar y dar acceso a los documentos digitales.

En las líneas de acción de la política se debe indicar, al menos, la necesidad de establecer los requisitos legales, técnicos, tecnológicos y de otra índole, la designación de los responsables de la preservación de los documentos, el desarrollo de un esquema de metadatos, así como disponer de los medios y recursos necesarios para facilitar, preservar y garantizar la integridad, autenticidad, confiabilidad y acceso a los activos de información.

4 La propuesta se basó en el en el Modelo OAIS, Norma UNE-ISO 14721: 2015, el modelo PLATTER, DPE Repository Planning Checklist and Guidance. DPED 3.2 April 2008, en la asesoría realizada por Jordi Serra Serra en la Universidad de Costa Rica y la experiencia del proyecto ARCA que es un Repositorio de Preservación de Documentos Digitales utilizado en el Archivo Nacional y desarrollado por la empresa Business Integrators Systems (BIS), del cual se recibió asesoría.

### 7.1.2. Definición del Archivo Digital

El Archivo Digital debe ser el responsable de preservar y garantizar el acceso, autenticidad e integridad de los documentos digitales y debe estar a cargo del Archivo Institucional con el apoyo técnico del Departamento de Tecnología, como responsable de la infraestructura y plataforma tecnológica necesaria para su funcionamiento continuo y eficiente y de su interoperabilidad con otros sistemas.

Para garantizar el adecuado funcionamiento del Archivo Digital, se recomienda conformar una Comisión de Preservación Digital (CPD en adelante) como órgano colegiado, encargado de coordinar, emitir y actualizar políticas, estrategias y lineamientos institucionales de preservación digital, debe ser capaz de asegurar los recursos económicos, tecnológicos y humanos necesarios.

La CPD debe estar integrada por el personal idóneo, que tenga el conocimiento técnico y la competencia para tomar decisiones estrategias a nivel institucional. La Comisión debe ser interdisciplinaria, considerando al menos las áreas de administración, informática y derecho y liderado por el responsable del Archivo Institucional.

El funcionario encargado de administrar el Archivo Digital, conocido como Senior Information Risk Owner (en adelante SIRO por sus siglas en inglés), debe tener la capacidad para dirigir, liderar, crear procedimientos, analizar los riesgos de la información y de continuidad digital del servicio; con el fin de garantizar el acceso, la preservación y la seguridad de la información comprensible en el tiempo.

La institución debe contar con un plan de capacitación permanente para el personal involucrado y un plan prevención contra desastres, que incluya un procedimiento de salvamento. Asimismo, debe contar con un protocolo de acción y un plan de emergencias en caso de desastre, que asegure la integridad del Archivo Digital, proteja la continuidad e integridad de los activos de información y restablezca los servicios que se brindan.

### 7.1.3. Plan de Datos

El Plan de Datos consiste en definir las características de los documentos y la información a preservar en el Archivo Digital, para esta tarea se deben aplicar las directrices de la Comisión

Nacional de Selección y Eliminación de Documentos (CNSED) y del Comité Institucional de Selección y Eliminación de Documentos (CISED).

El Archivo Digital gestionará la información requerida para los tres tipos de paquetes/ contenedores de información: el que se utiliza para la transferencia (*SIP*), el que se conserva en los repositorios (*AIP*) y el que se genera para consumo producto de una consulta (*DIP*), según lo que establece el Modelo OAIS, a saber:

Paquete de Transferencia de Información (*SIP*)

El *SIP* (Submissión Information Package, por sus siglas en inglés) es la información de contenido y descripción de los documentos que se ingresa al Archivo Digital, y que es utilizada para la construcción o actualización del paquete de información de archivo o *AIP* (Archival Information Package).

El *SIP* puede representar dos tipos de objeto con propiedades y funciones diferentes, puede ser la información y descripción de un determinado documento digital, junto con los datos de contexto y localización; o puede referirse a un conjunto de paquetes de información y descripción de un documento, que se envían a un repositorio. Para este caso, contendría la información, descripción autenticidad, integridad y localización de cada uno de los paquetes *SIP*, de una determinada transferencia, típicamente transportados en un solo fichero comprimido.

Paquete de Información de Archivo (*AIP*)

El *AIP* (*Archival Information Package, por sus siglas en inglés*) es el paquete de información que almacenará el Archivo Digital y es el mecanismo para contener la información y ejecutar los procesos de preservación.

El *AIP* contiene distintos tipos de datos, a saber: la información de contenido, la información descriptiva y de relaciones, la información de conservación asociada, incluidas las modificaciones necesarias para ser almacenado, y el fichero mismo auto-contenido, representado , preferiblemente usando como base la estructura METS con estructuras de nombres de nodos que cumplan las normas internacionales que les competen, para garantizar su usabilidad en el tiempo y la protección de la información de contexto,

protegido con un sistema confiable de aseguramiento de la información, como la firma digital avanzada XAdES X-L.

Paquete de Consulta de Información (*DIP*)

El *DIP* (Dissemination Information Packagepor sus siglas en inglés) es un paquete de información derivado del *AIP*, para distribuir el contenido digital que es consultado por los usuarios/sistemas que tienen acceso al Archivo Digital. La información de empaquetado va a depender de las necesidades identificadas y de los contratos de servicio con los sistemas consultantes.

### 7.1.4. Plan de Ingreso

El Plan de Ingreso es el proceso de transferencias de los documentos digitales, por lo que se deben establecer los servicios y funciones para recibir los paquetes *SIP* e identificar los documentos que van a formar parte del Archivo Digital, se debe definir los formatos admitidos que se van a utilizar en el Archivo Digital, con el fin de normalizarlos. Asimismo, se deberán utilizar esquemas de metadatos basados en estándares mundiales o apoyados por la normativa nacional, con el fin de conservar el contexto, y de garantizar la integridad, preservación y autenticidad.

El proceso de transferencia se debe realizar de manera normalizada, según se establece en la declaración de las reglas de transferencia establecidas en el documento denominado como *Protocolo de Transferencia*, que se hace por Serie Documental o por Sistema Institucional, con el fin de establecer la estructura, contenido y forma.

El ingreso de documentos al Archivo Digital se realizará por medio de transferencias automáticas o asistidas, pero siempre por los canales definidos y se podrán realizar de forma regular en un plazo acordado en el *Protocolo*, para lo cual debe especificarse el detalle y el método (*push o pull*).

El *Protocolo de Transferencia* debe tener al menos la información relacionada con: el 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, plazos de conservación, propiedades significativas coleccionables, derechos de uso y acceso y la fecha de vigencia del protocolo.

El *Protocolo de Transferencia* se debe actualizar al menos cada 5 años, o cuando exista algún cambio que pueda provocar la caducidad del protocolo; por ejemplo, una modificación del sistema de información, de la infraestructura tecnológica del Archivo Digital, de los valores y la significación, de la normativa, de los plazos de vigencia de los documentos o de los derechos de uso y distribución de la información.

### 7.1.5. 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.

Este Plan incluye el establecimiento de los servicios y la plataforma para el almacenamiento, mantenimiento y recuperación de los *AIP*. Las funciones de almacenamiento deben incluir la recepción de los *SIP* desde el ingreso, para que al ser procesados se añadan al almacenamiento permanente. Asimismo, se deben aplicar rutinas para la detección de errores, habilitar los medios de prevención en caso de desastres y proporcionar el acceso a la información.

Las funciones de conservación incluyen:

- Elaborar estrategias y planes de conservación, para asegurar que los documentos y los datos almacenados permanezcan íntegros, auténticos y accesibles en el tiempo.
- Evaluar el funcionamiento del Archivo Digital.
- Desarrollar planes de migración.
- Aplicar procesos de migración.
- Diseñar las plantillas de los paquetes de información.
- Controlar los documentos, es decir, verificar la cantidad y volumen custodiados, metadatos asociados, valores que permiten la interpretación de los códigos, entre otros.
- Realizar análisis de riesgos y control del entorno tecnológico.

- Monitorear la tecnología, por ejemplo, en caso de obsolescencia tecnológica.
- Realizar transformaciones de formato programadas.

Los documentos conservados por el Archivo Digital tendrán una representación tecnológica vigente, el SIRO deberá establecer cuáles formatos serán conservados y cuáles formatos deben transformarse para garantizar su vigencia. Para ello debe aplicar revisiones periódicas de los formatos en custodia y su posible renovación cuando las condiciones lo ameriten.

Las modificaciones se deben realizar únicamente con el fin de asegurar su acceso en el tiempo, siempre garantizando la integridad y autenticidad del documento mediante las técnicas que se consideren necesarias. La más común es la extracción y conservación de las propiedades significativas en los metadatos y estructuras correspondientes (metadatos del diccionario PREMIS en la estructura amdSec del contenedor METS). La apariencia y funcionalidades de un documento podrían cambiar producto de las transformaciones de formato, de acuerdo con los parámetros establecidos en el protocolo de transferencia correspondiente.

El SIRO debe poder identificar tendencias tecnológicas emergentes que podrían ser motivo de obsolescencia de los documentos en custodia en el Archivo Digital, e impedir, potencialmente, el acceso y la preservación en el tiempo de los documentos, así como de la información custodiada; en tal circunstancia el SIRO deberá disponer las contramedidas que considere oportunas para prevenir su afectación.

Para la detección del riesgo de obsolescencia tecnológica se debe:

- Contar con servicios de alerta (suscripción).
- Exploración de formatos.
- Verificación de lectura y/o ejecución de una muestra significativa de los formatos conservados.

En el caso de que se confirme un riesgo, el SIRO deberá elaborar un informe que contenga:

- Cantidad de *AIP* y de representaciones tecnológicas afectadas.
- Características técnicas del formato afectado.
- Las series documentales afectadas y las propiedades significativas en riesgo para el formato de fichero afectado.

- Los sistemas de información que transfieren afectaciones y la eventual necesidad de modificar los conectores para las transferencias.
- Los posibles formatos de destino en caso de conversión, las características de los nuevos formatos, las herramientas que se deben utilizar y las propiedades significativas que se van a conservar, así como las que podrían resultar modificadas.
- Propuesta de actualización del Protocolo de Transferencia.
- Costo total del proceso de migración/conversión.
- Resultados de los prototipos y alertas sobre tecnología.
- Planes de migración y conversión de formatos.

### 7.1.6. Plan de Acceso

En el Plan de acceso 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 Archivo Digital.

El Archivo Institucional debe establecer el plan y el conjunto de reglas que aplique los 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.

Por su parte, el Archivo Digital debe tener la capacidad de brindar información a través interfaces de consulta para usuarios internos y externos y servicios de interoperabilidad para que aplicaciones institucionales se integren con el Archivo Digital, mediante un sistema de consumo que facilite la visualización en línea de los documentos, la descarga (cuando sea permitido) y la reprografía certificada (los documentos obtenidos por este medio tendrán carácter de copia auténtica.

### 7.1.7. Plan de Tecnología

La infraestructura del Archivo Digital deberá ajustarse a las necesidades de almacenamiento, procesamiento, seguridad y comunicaciones, ser escalable y redundante, utilizando *software* y equipo con tecnología de vanguardia, pero confiable.

La infraestructura del Archivo Digital es responsabilidad de la Dirección de Tecnología de la organización y deberá garantizar la autenticidad, integridad y disponibilidad de los servicios y plataforma requerida para la operación del Archivo Digital.

Como parte de los mecanismos de seguridad que debe implementar un Archivo Digital, es necesario contar con un recurso que permita prevenir y/o detectar modificaciones hechas a los documentos o a los datos bajo custodia, y tener a disposición un mecanismo que permita restaurar el activo manipulado a su estado primero.

Se debe contar con pistas de auditoría, incluyendo los registros de los eventos del sistema, los cuales también deben estar provistos de un mecanismo que permita asegurar su integridad, mediante la protección de un algoritmo criptográfico.

Es importante que el Archivo Digital cuente con un programa de verificaciones de autenticidad e integridad, y de ensayos de los procesos de recuperación y continuidad de servicio. Estas revisiones y pruebas deberán generar informes de resultado, que se usarán como insumo para gestionar la protección contra ataques informáticos y para la configuración de los procesos de recuperación en caso de desastres.

Cualquier evento asociado con el ciclo de vida de los documentos se debe documentar usando los elementos de la estructura de metadatos del *AIP* diseñados para tal propósito, en el apartado de eventos del diccionario PREMIS.

Con el fin de certificar la seguridad de la información se deben realizar las siguientes acciones:

- Verificaciones de integridad mediante recalcular y comparar el hash de todos los paquetes de información, al menos una vez cada ciclo completo de pruebas.
- Verificaciones periódicas de la existencia de errores en los dispositivos de memoria de los soportes de almacenamiento.
- Llevar un registro de todos los incidentes de seguridad, junto con la medida adoptada para resolverlos, el tiempo de resolución y las consecuencias que tuvo en el objeto afectado.
- Elaborar un informe periódico de las incidencias.

Asimismo, se debe mantener copias de seguridad incrementales en un soporte no alterable, que deben realizarse con periodicidad diaria (las incrementales) y semanal para la copia base. Adicionalmente, es necesario que exista 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 cifrado y ocultamiento, para proteger la información en el tránsito, o cuando los almacenamientos sean compartidos por otras aplicaciones.

### 7.1.8. Plan de Continuidad

Para garantizar la disponibilidad y la operación ininterrumpida del Archivo Digital se debe mantener un Plan de Continuidad, elaborado y actualizado por el Departamento de Tecnología, con el propósito de estar preparados en caso de interrupciones largas del servicio causadas por factores internos o externos sin control y con el fin de restablecer los servicios, en la mayor medida posible, en un tiempo mínimo. Dicho plan abarca todos los sitios e instalaciones de la Infraestructura Tecnológica y los componentes de los servicios de *software* hospedados en ellos.

El plan de continuidad debe gestionarse de acuerdo a las mejores prácticas establecidas en la norma internacional ISO 27001.

## 7.2. MODELO FUNCIONAL Y TECNOLÓGICO DEL ARCHIVO DIGITAL

### 7.2.1. Modelo funcional del Archivo Digital

Los requisitos funcionales caracterizan los elementos que se deben incluir en el repositorio digital. De acuerdo con el Modelo OAIS (Norma UNE-ISO 14721, págs. 41-57) son 6 entidades funcionales relacionadas, a saber:

- Entidad funcional de Ingreso.
- Entidad funcional de Almacenamiento de Archivo.
- Entidad funcional de Gestión de Datos.
- Entidad funcional de Administración.
- Entidad funcional de Planificación de la Conservación.
- Entidad funcional de Acceso.

Ingreso

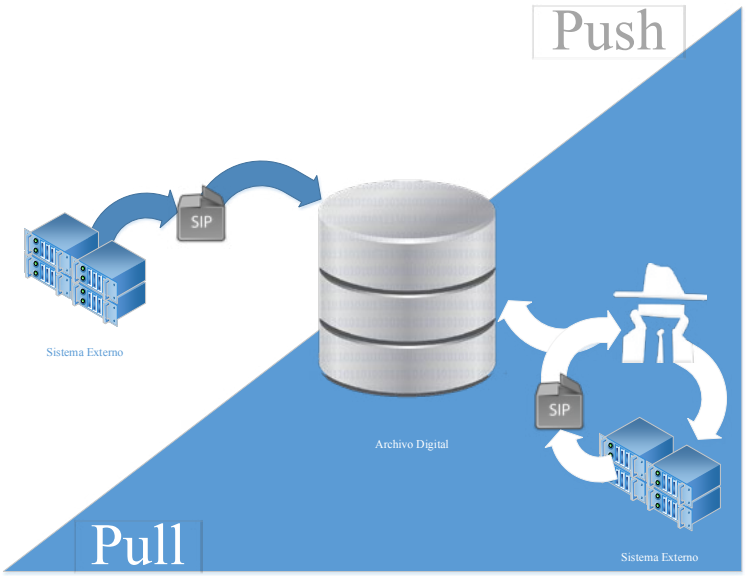
Son los servicios y funciones con los que debe contar el repositorio digital para recibir y obtener los Paquetes *SIP*. La función de ingreso sirve como interfaz externa del repositorio con las instancias que producen los documentos, para habilitarles el envío de estos para su almacenamiento y conservación.

Dentro de los servicios y funciones están los siguientes:

- Identificar los documentos que deben ingresar al Archivo Digital.
- Validar el esquema de metadatos obligatorios en el *SIP*.
- Recibir o recoger los *SIP* y aplicar control de calidad del mismo
- Generar los metadatos normalizados para convertir el *SIP* en *AIP*.
- Generar notificaciones y bitácoras correspondientes.

El procesamiento del *SIP* se puede iniciar de dos maneras: a) pull: el repositorio cuenta con un agente de "middleware" que "sale y recoge" el material, o b) push: el *SIP* se entrega en el repositorio para su procesamiento por parte del sistema u organismo productor original.

**FIGURA 2. Métodos pull y push**




Fuente: Elaboración propia.

Se recomienda que el *SIP* de cada documento se materialice mediante un único fichero, en formato XML, en una estructura codificada usando el esquema METS, que debe incluir los metadatos descriptivos de las unidades documentales que se transfieren al Archivo Digital, en los elementos identificados con la etiqueta <dmdSec>.

La forma de envío para el *SIP* debe implementar el uso de la firma digital en formato XAdES-T envelopping o superior, y utilizar un certificado de confianza para el dispositivo o aplicación del sistema receptor. Este mecanismo otorga garantía de autenticidad e integridad de los datos del *SIP* para el sistema receptor (repositorio), así como un control de versión de los datos mediante la fecha/hora de creación del *SIP*.

**Tabla 1. Procedimiento de transferencia (método push)**

| Nº | Agente | Acciones |
|---|---|---|
| 1 | Productor | Identificar los documentos a transferir. |
| 2 | Sistema/Productor | Preparar los documentos e información de contexto. |
| 3 | Sistema/Productor | Generar los metadatos descriptivos. |
| 4 | Interfaz/módulo para la Transferencia (Productor) | Encapsular y empaquetar los documentos y su información de contexto en contenedores *SIP*, aplicar la firma digital en formato XAdES-T envelopping para el envío del paquete *SIP*. |
| 5 | Interfaz/módulo para la Transferencia (Productor) | Crea un *SIP* compilatorio con la información de todos los *SIP* que representa cada documento, aplica la firma digital en formato XAdES-T envelopping para el envío para el paquete *SIP* y guarda el *SIP* compilatorio, los contenedores *SIP* de cada documento y los ficheros de documento (en caso de utilizar el método de referenciación) en un en un fichero comprimido de formato ZIPISO/IEC 21320-1:2015, que puede o no estar cifrado, de acuerdo al Protocolo de Transferencia establecido para el caso específico. |

| | | |
|---|---|---|
| 6 | Interfaz/módulo para la Transferencia (Productor) | Generar la lista de remisión (manifiesto) con la información de localización del archivo comprimido ZIP y la información para la validación de integridad y autenticidad. |
| 7 | Interfaz/módulo para la Transferencia (Productor) | Envía el manifiesto al repositorio para su procesamiento, también envía el paquete ZIP al dispositivo de almacenamiento convenido para su procesamiento y/o custodia. |
| 8 | Servicio para la recepción y procesamiento de Transferencias (Archivo Digital) | Recibe la lista de remisión “manifiesto”. |
| 9 | Servicio para la recepción y procesamiento de Transferencias (Archivo Digital) | Valida la identidad transferente:<br>• Obtiene el paquete de contenidos.<br>• Calcula y verifica el hash del paquete de contenidos.<br>• Aprueba o rechaza el paquete de contenidos, dependiendo de la validación de su integridad y autenticidad, acorde con la información declarada en el manifiesto. |

| | | |
|---|---|---|
| 10 | Servicio para la recepción y procesamiento de Transferencias (Archivo Digital) | Inicia el procesamiento de cada documento listado en el manifiesto de transferencia. Para cada uno se llevan a cabo los siguientes procesos:<br><br>• Valida el contenido, la estructura y la forma del *SIP* según lo establecido en el Protocolo de transferencia.<br>• Reconoce y valida los formatos de fichero para el documento electrónico recibido.<br>• Revisa la existencia de virus en el fichero referenciado o instancia el fichero a partir de su representación en base 64.<br>• Valida las firmas electrónicas existentes<br>• Aprueba o rechaza el documento, en ambos casos escribe una bitácora de la acción tomada, en caso de aprobación los eventos serán registrados posteriormente en los procesos de generación de metadatos de preservación, en caso de rechazo la causa de este será incluida en un informe que se hace llegar al contacto registrado de la unidad transferente. |
| 11 | Servicio de reconocimiento y conversión de formatos de fichero | Aplica las reglas de administración de formatos y preservación documental. También registra los metadatos de preservación correspondientes al evento de conversión de formato, si lo hubo. |
| 12 | Archivo Digital | Genera o extrae y guarda los metadatos de preservación (tecnológicos y de evento) y las propiedades significativas. |
| 13 | Archivo Digital | Aplica el esquema de metadatos final del *AIP* y guarda los metadatos recibidos y creados en la estructura pre-establecida. |
| 14 | Archivo Digital | Conforma y registra el Paquete de Información de Archivo (*AIP*). |
| 15 | Archivo Digital | Aplica protección de la información del *AIP*, calcula llaves criptográficas para garantizar la autenticidad e integridad de los documentos . |

| | | |
|---|---|---|
| 16 | Archivo Digital | Crea el asiento correspondiente en el registro de transferencias y actualiza la información en los índices de búsqueda y los sistemas relacionados con la consulta documental. |
| 17 | Servicio o aplicación de firma/sellado electrónico. | Aplica la firma digital en formato XAdES-XL envelopping a todo el paquete creado, esto genera la versión final del *AIP* y procede a su almacenamiento. |
| 18 | Archivo Digital | Notifica el ingreso de la transferencia al productor y/o responsable del sistema institucional mediante una línea con el detalle en un informe sumario. |

Fuente: Elaboración propia.

**Tabla 2. Procedimiento de adquisición (método pull)**

| Nº | Agente | Acciones |
|---|---|---|
| 1 | Productor | Identifica los documentos a transferir. El productor debe establecer de forma previa un contrato con el Archivo Digital que le permita a este último conocer cuáles documentos serán transferidos. |
| 2 | Productor / Archivo Digital | Establece el canal para acceder a los documentos identificados para su conservación, y los orígenes y permisos de acceso a la información de contexto. |
| 3 | Agente “middleware” del Archivo Digital | Establece comunicación con los canales definidos por el productor para la recolección de los documentos y genera los metadatos descriptivos y la información de contexto a partir de los orígenes de datos establecidos |

| | | |
|---|---|---|
| 4 | Agente "middleware" del Archivo Digital | Encapsula y empaqueta los documentos y su información de contexto en contenedores *SIP*, aplica la firma digital en formato XAdES-T envelopping para el envío del paquete *SIP*; el certificado digital firmante deberá aplicar el método que permita reconocer el origen de un paquete "*pull*", el paquete debe identificarse como de origen "*pull*", pero la validación de esto dependerá de la autenticidad de la firma digital del paquete. |
| 5 | Servicio para la recepción y procesamiento de Transferencias (Archivo Digital) | Reconoce y valida la procedencia, e identifica el paquete como de origen "*pull*" para aplicar un mecanismo abreviado de carga sin paquete *SIP* compilatorio. |
| 6 | Servicio para la recepción y procesamiento de Transferencias (Archivo Digital) | Inicia el procesamiento del documento mediante los siguientes procesos:<br>• Valida el contenido, la estructura y la forma del *SIP* según lo establecido en el *Protocolo de Transferencia*.<br>• Reconoce y valida los formatos de fichero para el documento electrónico recibido.<br>• Revisa la existencia de virus en el fichero referenciado o instancia el fichero a partir de su representación en base64.<br>• Valida las firmas electrónicas existentes<br>• Aprueba o rechaza el documento, con la bitácora y generación de metadatos correspondiente. |
| 7 | Servicio de reconocimiento y conversión de formatos de fichero | Aplica las reglas de administración de formatos y preservación documental. Registra el nuevo formato como el formato disponible y guarda el documento original. También registra los metadatos de preservación correspondientes al evento de conversión de formato, si lo hubo. |

| | | |
|---|---|---|
| 8 | Archivo Digital | Genera, extrae y guarda los metadatos de preservación (tecnológicos y de evento) y las propiedades significativas. |
| 9 | Archivo Digital | Aplica el esquema de metadatos final del *AIP* y guarda los metadatos recibidos y creados en la estructura pre-establecida. |
| 10 | Archivo Digital | Conforma y registra el Paquete de Información Archivística (*AIP*). |
| 11 | Archivo Digital | Aplica protección de la información del *AIP*, calcula llaves criptográficas para garantizar la autenticidad e integridad de los documentos. |
| 12 | Archivo Digital | Crea el asiento correspondiente en el registro de transferencias y actualiza la información en los índices de búsqueda y los sistemas relacionados con la consulta documental. |
| 13 | Servicio o aplicación de firma/sellado electrónico. | Aplica la firma digital en formato XAdES-XLenvelopping a todo el paquete creado, esto genera la versión final del *AIP* y procede a su almacenamiento en el soporte definido. |

Fuente: Elaboración propia

Almacenamiento

Este elemento provee los servicios y funciones relacionados con el almacenamiento, mantenimiento y recuperación de los *AIP*, seguridad de los activos de información, actualización de soporte, control de fallas y detección de errores, entre otros.

Gestión de Datos

La Gestión de datos provee los servicios y funciones relacionados con el ingreso de datos y su finalidad es mantener y acceder tanto a la información descriptiva con la que se identifican y documentan los fondos y subfondos de archivo, como a los datos administrativos empleados para gestionar el Archivo Digital y gestionar los índices de búsqueda.

Administración

Contempla los servicios relacionados con el funcionamiento global del sistema, que incluye las normas del Archivo y mantener la configuración de la gestión del sistema, así como su plataforma de *hardware* y de *software*, controlar las funciones del archivo, implementar mejoras, mantenimiento de las políticas, entre otros.

Planificación de la Conservación

Es responsable de fijar la estrategia de conservación del repositorio, proporciona los servicios y funciones de control del entorno del Archivo Digital, con recomendaciones y planes de conservación para asegurar que la información almacenada permanezca accesible a largo plazo, e inteligible, para la comunidad específica, incluso cuando el entorno automatizado original devenga obsoleto.

Una parte importante de la planificación de la conservación es la *administración de formatos,* cuyo principal objetivo es mantener en constante revisión los cambios tecnológicos y la obsolescencia del formato utilizado, para aplicar la conversión o transformación en el momento oportuno.

Por lo que, el Archivo Digital debe identificar, administrar y normalizar los formatos que ingresan. Para ello debe tener la información propia de los formatos admitidos/permitidos en el repositorio, y la lista de los formatos no admitidos, así como una regla que indique su respectivo formato de destino para la conversión.

El SIRO es el funcionario encargado de la vigilancia tecnológica, debe conocer con exactitud las características de los formatos de fichero existentes, identificando las necesidades de conversión, ya que los formatos custodiados por el Archivo Digital deben estar normalizados y actualizados. Para ello, puede hacer evaluaciones de los formatos existentes utilizando las herramientas: Shotgun del proyecto PLANETS, DROID, JHOVE, XENA, entre otros.

Cuando se aplique la conversión o transformación de formatos, el Archivo Digital debe verificar que el objeto transferido declara adecuadamente su tipo de formato, conocido como tipo “MIME” y este se encuentra dentro de los formatos administrados/permitidos.

En el *AIP* se almacenarán el(os) formato(s) seleccionados para preservación y el *DIP* deberá tener una funcionalidad que le permita convertir los formatos para difusión (copia de consulta), de acuerdo con lo que se establezca en el contrato de consumo, pero en este caso no serán almacenados de forma permanente, por lo que se crean bajo demanda cada vez que se solicite un documento y se destruyen posteriormente, para garantizar el mejor aprovechamiento de los recursos de almacenamiento.

Acceso

El componente de Acceso aporta acciones de apoyo a los usuarios para determinar la existencia, descripción, localización y disponibilidad de la información almacenada, y permite a los usuarios solicitar y recibir productos de información, el control de las listas de acceso por serie documental y las excepciones necesarias de acceso a expedientes o documentos con necesidades especiales, el mantenimiento y la mejora constante de la interfaz de búsqueda y participa en la elaboración de contratos de consumo de paquetes de difusión (*DIP*) personalizados.

### 7.2.2. Modelo Tecnológico del Archivo Digital

El escenario ideal se plantea alrededor de una solución de archivo digital que brinde al menos los siguientes servicios y funcionalidades:

- El servicio para la recepción del *SIP* implementado de manera híbrida, un servicio para la recepción de paquetes maestros de tipo push y un servicio para la recepción de envío de información granular desde agentes para el tipo pull. En el primero, el repositorio procesa un paquete que contiene múltiples documentos en cada transferencia y en el segundo, un agente realiza transferencias de documentos obteniéndolos de otras bases de datos o sistemas, pieza por pieza.
- Creación y gestión de una estructura de organización que refleje el cuadro de clasificación archivístico indicado por el productor, para catalogar cada pieza documental.
- Creación y gestión de contenedores asegurables de archivos para cada unidad documental compuesta o expediente, que garantice el aseguramiento de sus piezas documentales y del orden de ingreso de estas.

- Servicio de detección de virus y amenazas de malware en los ficheros transferidos.
- Comprobación de autenticidad e integridad de los documentos cuando existan los medios disponibles, tal como las firmas digitales en formatos de alta longevidad o los cálculos realizados mediante números característicos obtenidos de algoritmos preestablecidos.
- Servicio de reconocimiento y conversión de formatos de fichero por medio de la llave de identidad del contenido o tipo MIME.
- Gestión de protocolos para la administración y acceso, para garantizar la seguridad de la información.
- Utilización de esquemas de metadatos basados en la codificación estándar para las normativas internacionales de descripción ISAD-G e ISAAR-CPF y el diccionario de preservación PREMIS.
- Verificación del documento digital mediante el número característico obtenido de algoritmos de comprobación MD5.
- Estructura de información del *AIP* mediante el estándar METS.
- Operación asincrónica para el transporte, extracción de propiedades significativas de preservación digital, aseguramiento, sellado y conformación de paquetes *AIP*.
- Firma y sellado de tiempo por una autoridad de confianza y competente de valor nacional.
- Servicio de búsquedas integrable a otros desarrollos informáticos capaces de retornar paquetes personalizables de tipo *DIP* y con capacidad de realizar reprografías.
- Control de acceso a los documentos en custodia en los niveles de serie documental, unidad documental compuesta o expediente y documento, aplicable a todas las formas de consumo de información.
- Gestión de reglas de trazabilidad personalizables y notificación de los distintos eventos y operaciones del sistema.
- Interfaz web para la configuración, establecimiento de las políticas de Descripción Documental, Acceso y Confidencialidad, Administración, Transformación y Reconocimiento de Formato de Ficheros Digitales, y demás funciones del Archivo Digital detalladas en esta lista de servicios y funcionalidades.

En cumplimiento de la Norma ISO 14641:2012 se recomienda crear y conservar un manual de descripción técnica del sistema de información que debe contener al menos:

- una lista de los componentes *hardware* del sistema de información;
- la distribución e interacción de los componentes del sistema en la red de datos, así como una descripción de las conexiones y del equipamiento de seguridad;
- un modelo de la arquitectura de datos de los objetos de información y sus relaciones;
- una lista de productos de *software* que interactúan y documentación relacionada;
- una lista de las aplicaciones *software* personalizadas con su fichero del diseño y de la arquitectura, su código fuente o una prueba de su depósito bajo custodia, cuando sea posible (Norma ISO 14641:2012, pág. 13).

Es necesario garantizar las mejores condiciones de operación de los equipos que hospedan los servicios de la solución en el centro de datos de las instituciones, en concordancia con el estándar ANSI/TIA-942 Telecommunications Infrastructure Standard for Data Centers, operando, como mínimo, bajo el modelo de fuentes paralelas de poder ininterrumpido o esquema N+1 (Tier3) o preferiblemente bajo el modelo de redundancia 2(N+1) (Tier4) para todos los servicios y componentes del sistema incluyendo los servicios de refrigeración.

Debe incluirse los servicios del repositorio como parte del plan de continuidad de negocio de la institución o BCP (Business Contingency Plan), estos servicios deben replicarse en un sitio alterno que permita la continuidad de las operaciones y consultas, así como la salvaguarda de los activos de información ante ciberincidentes, y como medida en caso de catástrofe. El plan de continuidad de negocio deberá establecer al menos los siguientes elementos:

- Identificación de los Activos.
- Valoración de Riesgos.
- Establecimiento de Estrategias de Continuidad.
- Establecimiento de roles, responsabilidades y procedimientos.
- Estrategias, Procedimientos y Tiempo Meta de Recuperación (Recovery Time Objective, RTO).
- Manual de Procedimientos de Continuidad.
- Plan de pruebas con calendario de cumplimiento, proceso de análisis de resultados y mejora continua.

El sitio alterno debe estar ubicado, idealmente, a una distancia no menor de 150 Kilómetros del sitio principal y deberá contarse con medios de comunicación redundantes entre ambas instalaciones.

La seguridad física del centro de datos debe integrar un conjunto de políticas, procedimientos y dispositivos que permita asegurar protección de alto nivel. Debe establecerse medidas de seguridad para el perímetro del centro de datos, para sus instalaciones físicas, para el centro de datos mismo, y si es posible, a nivel de los gabinetes que contienen los servidores que hospedan la solución, las comunicaciones entre los equipos servidor deben estar protegidas por protocolos de seguridad como IPSec, de manera que evite la intrusión de equipos indeseados.

El acceso físico al centro de datos debe ser restringido y debe quedar registrado, así como su duración, propósito y tiempo de salida, el centro de datos debe estar protegido por un circuito cerrado de televisión que registre la actividad que ocurre dentro de él y permita seguir los movimientos de las personas que tienen acceso físico. Estas grabaciones podrán reproducirse para identificar y documentar eventos, con el fin de tomar las medidas oportunas.

El centro de datos debe contar con sistemas de detección de humedad e inundaciones y un sistema avanzado de control de incendios que no dañe los equipos que no están siendo afectados por el siniestro.

Debe separarse física y lógicamente la red de almacenamiento de las redes de acceso a usuarios, permitiendo solo que las terminales autorizadas tengan acceso a los almacenes de información y solo a través de los protocolos que la solución requiera. Debe monitorearse el tráfico de paquetes mediante un sistema de prevención de intrusos (Intrusion Prevention System, IPS por sus siglas en inglés) para prevenir en tiempo real cualquier incidente de seguridad.

Los sistemas de almacenamiento requieren contar con medios redundantes que soporten el fallo de los dispositivos de los que están compuestos sin pérdida de información, conocidos como Matrices Redundantes de Discos Independientes (Redundant Array of Independent Disks o RAID por sus siglas en inglés), la configuración de estas matrices de redundancia

deberán estar acordes a las recomendaciones del fabricante, en lo que se refiere a condiciones de operación, permitiendo la configuración de unidades lógicas que garanticen la optimización de los almacenes de datos.

La solución de *software* de archivo digital deberá estar cubierta por un servicio de mantenimiento y soporte 24x7x365. Es importante establecer el nivel deseado de calidad para el servicio de soporte y que este se plasme en un acuerdo de nivel de servicio (Service Level Agreement o SLA por sus siglas en inglés), que deberán suscribir el Archivo Digital y el proveedor para cada servicio relacionado con la solución, incluyendo su plataforma tecnológica, infraestructura y comunicaciones, independientemente de si las partes pertenecen a la misma organización o no.

Requerimientos de arquitectura tecnológica

- El *software* de Archivo Digital que se elija debe operar en conformidad con los requisitos que establece el Modelo OAIS, cuyos principios ya han sido desarrollados en apartados previos.
- El *software* de Archivo Digital deberá operar empleando el paradigma de la arquitectura orientada a servicios SOA, de modo que esté habilitado para implementar interfaces con el fin de que sea interoperable con sistemas dentro y fuera de la institución, sin incurrir en procesos de alta complejidad.
- Debe permitir el crecimiento horizontal y vertical, de forma escalonada hasta cumplir con las necesidades de la institución.
- Debe garantizar en todo momento el control de acceso a la información en custodia con la misma configuración y seguridad, independientemente de la interfaz que solicita el acceso.

Almacenamiento

El Archivo Digital debe contar con una base de datos relacional para la información de los objetos de descripción y su membresía, que permita asegurar los contenidos de las entidades débiles, debe contar también con un servicio especializado para realizar las búsquedas que utilice un motor de Índice de Texto, las búsquedas deben contar con análisis de léxico, análisis morfológico y puntaje de clasificación mediante algoritmos para cuantificar en qué medida un determinado registro coincide con palabras clave de búsqueda, ambos servicios deben poder ser hospedados localmente en el centro de datos de la organización y/o en la nube.

Presupuesto

Un componente vital de todo proceso institucional es la asignación de presupuesto, un Archivo Digital debe verse como una necesidad de toda la institución, y no como parte de un centro de costos específico, como un departamento, por ello se recomienda que su autoridad esté a cargo de la Comisión de Preservación Digital. De acuerdo con lo que establece la Política de Preservación Digital, la institución debe gestionar los recursos necesarios para preservar los documentos de forma íntegra, auténtica, fiable y accesible a través del tiempo.

Como parte de la planificación de la institución se debe contemplar los recursos financieros previstos para la ejecución, mantenimiento y almacenamiento, del Archivo Digital, e incorporar una previsión al costo de adaptación para posibles migraciones o cambios en la tecnología que impliquen sustituciones de los equipos de la plataforma tecnológica.

Basado en una proyección, de acuerdo con la oferta en el mercado, se puede estimar el costo de la plataforma tecnológica y los recursos necesarios para implementar y hospedar la solución de archivo digital, esta estimación podrá cambiar según los dos factores indicados a continuación:

- Volumen de datos: Existe una relación directamente proporcional entre el volumen de datos en resguardo y el costo del almacenamiento, a mayor volumen de activos de información en custodia, mayor es el costo para resguardarlos, en el caso de la implementación en el centro de datos de la organización este costo puede ser representado por costos escalonados entre los distintos volúmenes.
- Cantidad de Consultas: La cantidad de consultas incide directamente en la capacidad de procesamiento y la cantidad de nodos de servicio que una solución de informática requiere para satisfacer la demanda, de manera que, a mayor cantidad de consultas, mayor requerimiento de recursos.

Con respecto al *software* de archivo digital una institución tiene dos alternativas, desarrollar un sistema de archivo digital con las especificaciones requeridas, o bien adquirir uno que las cumpla.

En el caso del desarrollo, este puede ser interno o externo, para ambos casos deberá definirse un equipo de trabajo que lidere el proyecto y las características y costos de

implementación, las cuales irán surgiendo con el tiempo como producto del trabajo de este equipo multidisciplinario.

El cálculo referente a la configuración de plataforma tecnológica y requerimientos de la solución se cuantifica a través de las especificaciones que los fabricantes indiquen para la carga y condiciones de uso proyectado, de manera que se obtenga un resultado más acercado al costo real de implementación y operación, el cuál debe delimitarse por un plazo de tiempo definido, idealmente entre tres y cinco años, debido a la evolución tecnológica, tanto de *hardware* como de *software*, incluyendo el motor de base de datos utilizado.

Finalmente, para la proyección del costo de la solución de Archivo Digital debe considerarse costos de mantenimiento, aunque se utilice código libre, que no representa costo económico de licenciamiento, pero que insta a que la institución dedique personal para el soporte y la mejora del producto para la comunidad, por lo que podría asociarse de forma indirecta al salario de los profesionales dedicados al proyecto.

Asimismo, debe analizarse la opción de Infraestructura como Servicio (Infrastructure as a Service o IaaS, por sus siglas en inglés), una modalidad que permite implementar la solución de archivo digital en la nube. Es necesario evaluar esta iniciativa con mucho cuidado, aunque se minimiza el riesgo de pérdida de información accidental, debido a la garantía de replicación geográfica de datos, sí existe el riesgo de pérdida de la información por no contar con la liquidez para hacer frente al pago de las obligaciones de arrendamiento en el plazo contractual establecido.

La principal ventaja que ofrece una implementación en la nube es la desvinculación con los problemas de la gestión de un centro de datos, el suministro de energía, la refrigeración, la falla de componentes electrónicos, la actualización de los entornos de plataforma, la gestión de las comunicaciones y demás servicios facilitadores, por lo que es una tendencia de alto crecimiento a nivel mundial, y por tal razón se debe hacer una proyección de sus costos, pero esta vez solo a un plazo de 3 años, pues es el plazo máximo al que se obtiene un beneficio económico en forma de un descuento.

En lo relativo a las características del servicio de firma para sello institucional se recomienda un servidor dedicado, con la desmaterialización del certificado digital institucional, producto

del cambio en el reglamento para éstos que ahora permite utilizarlo en dispositivos HSM virtuales, los costos del servicio han disminuido y su capacidad de operación se ha maximizado, haciendo más factible su implementación.

La naturaleza de la propuesta de Archivo Digital exige el uso de la firma digital de alta longevidad XAdES XL como mecanismo de protección de los paquetes de información de archivo (*AIP*) y en este mecanismo de seguridad recae gran parte de la protección de los activos de información durante la custodia.

La firma digital es un proceso confiable, económico y de fácil operación cuyo valor está garantizado por la Ley 8454, sus características no sólo son compatibles sino ideales a la estructura de implementación del Modelo OAIS, por lo tanto, los recientes cambios en el reglamento de uso de los certificados institucionales para el así llamado "sello institucional" resultan de especial importancia como facilitadores de la implementación de Archivos Digitales seguros para las instituciones de nuestro país.

# 8. CONCLUSIONES

La sociedad actual se caracteriza por una producción masiva de información, por demandar su acceso y exigir un mejor servicio, tanto de las instituciones del Estado como de las empresas privadas; los archivos son los entes posibilitadores del acceso oportuno, exacto y veraz de la información que genera conocimiento, debido a que los documentos, sin importar el soporte, son uno de los recursos y activos más importantes en las organizaciones.

Disponer de la información en el momento oportuno, permite una propicia gestión institucional, ahorro de recursos (económico y de tiempo), servicios de calidad y la salvaguarda del patrimonio documental, estas realidades no sólo no cambian en el ámbito digital, sino que se potencian con la velocidad y facilidad de uso de los nuevos soportes.

El avance tecnológico, como catalizador de cambio, hace que nuestra sociedad se transforme aceleradamente y que las instituciones deban adaptarse de manera oportuna, para mejorar sus servicios y ser más eficientes, mediante un sano equilibrio entre continuidad y la

transformación, que les permita la mejora sostenible y continua de sus procesos y de los trámites administrativos.

La tecnología como herramienta trae consigo muchas ventajas, su uso como medio de soporte de información es una de ellas, principalmente en lo que se refiere al acceso inmediato y concurrente de los documentos; aspecto que hoy día es necesario ver reflejado en las iniciativas de acceso a la información pública, en pro de los derechos de los ciudadanos, la transparencia y la rendición de cuentas. Indiscutiblemente, el uso de la tecnología como herramienta es un motor de desarrollo que, si se aplica adecuadamente, permite acercar a la ciudadanía, la institución y los servicios que ofrece, volviendo éstos últimos más eficientes, expeditos, oportunos y económicos.

En nuestro país, las instituciones se encuentran en una etapa de transición entre el soporte papel y el electrónico, por lo que es necesario que estén conscientes de los beneficios, pero también de los riesgos que implica; principalmente, los que conlleva la obsolescencia del medio digital de almacenamiento y del formato, así como el grado de garantía de la integridad y autenticidad de los objetos digitales.

La preservación digital representa uno de los desafíos impostergables que enfrenta la sociedad de la información. Ya que, nuestras instituciones se impregnan cada vez más de los cambios que trae consigo la revolución tecnológica, a fin de aprovechar sus ventajas, y no solo mantener la competitividad en una sociedad altamente tecnificada, sino conservar el liderazgo dentro de ella, para la organización y para todas las personas que confían nuestro estado de derecho, se evidencia la necesidad de contar con un Modelo de Preservación de Documentos Digitales.

En este sentido, el resultado de la investigación pretende colaborar en un problema actual, relevante y de alcance nacional, un reto irrefutable que las instituciones deben abordar de inmediato y de manera responsable; por lo que, es vital la implementación del modelo, ante la necesidad de contar con una herramienta confiable para administrar y conservar los objetos digitales que producen y reciben las organizaciones en el ejercicio de sus funciones, de manera que se asegure que sean auténticos, íntegros y usables a mediano y largo plazo.

Para ello, se requiere la creación de políticas, estrategias u otras disposiciones normativas para la preservación digital, mediante las que se deleguen y asignen las responsabilidades,

según las competencias de los involucrados en el proceso, con programas que generen los aspectos funcionales y técnicos requeridos, contar con 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.

Resulta clave para el establecimiento de un Archivo Digital implementar el Modelo OAIS, ya que es el referente internacional normalizado que define los elementos funcionales y técnicos, que permiten realizar las acciones necesarias para preservar los documentos digitales a largo plazo.

Queda establecido que un Archivo Digital tiene como objetivo preservar los documentos a través del tiempo y asegurar su acceso. La complejidad del desafío que plantea la obsolescencia tecnológica hace necesario contar con una gestión que resulta también compleja y especializada, mediante el intenso trabajo intelectual en lo referente a la modelación y el uso de las estrategias y las herramientas que implementa la metodología de los modelos de referencia OAIS, a fin de incrementar la probabilidad de contar con un acceso ininterrumpido a la información de documentos auténticos e íntegros, lo que convierte al Archivo Digital en la pieza fundamental e imprescindible de todo sistema de información archivística.

Es necesario aplicar las estrategias de preservación que le permita enfrentar los retos actuales y futuros, facilitando nuevos servicios y la preservación de la herencia en soporte digital, aprovechando las tecnologías de la información y la comunicación, con los medios y recursos necesarios para facilitar, preservar y garantizar el acceso a la información a través del tiempo.

El desarrollo de un esquema de metadatos es imprescindible para cerciorarse de la conservación de la información de contexto y las propiedades significativas que permitan asegurar, a través del tiempo y de los cambios tecnológicos, la continua accesibilidad, usabilidad, significación y valor probatorio de los objetos digitales bajo su custodia, así como el consumo e integración con otros sistemas a través de la normalización y el cumplimiento de estándares internacionales.

La propuesta de modelo de preservación digital pretende que los documentos digitales producidos en el ejercicio de sus funciones de las organización en general, y en las instituciones

de educación en particular, sean auténticos, íntegros y usables a mediano y largo plazo, así como potenciar la interoperabilidad entre sistemas y erradicar el problema de las islas de información; pero, además, dicha propuesta se constituye en un marco orientador y de referencia para la administración nacional, con el propósito de asegurar la preservación de los documentos digitales de las entidades públicas costarricenses.

# 9. BIBLIOGRAFÍA

Asociación Española de Normalización y Certificación. (2008). *Norma UNE-ISO/TR 18492: Conservación a largo plazo de la información basada en documentos.* España: AENOR.

Asociación Española de Normalización y Certificación. (2013). *Norma UNE-ISO/TR 17068:2013 Repositorio de tercero de confianza para documentos electrónicos. Información y documentación.* España: AENOR.

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 14641-1:2015 Archivo electrónico. Parte 1: Especificaciones para el diseño y funcionamiento de un sistema de información para la preservación de información digital.* 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.

Asociación Española de Normalización y Certificación. (2016). *Norma Internacional ISO 15489-1:2016 Información y documentación. Gestión de documentos. Parte 1: Conceptos y principios.* España: AENOR.

Asociación Española de Normalización y Certificación. (2017). *Norma UNE-ISO 16363:2017 Sistemas de transferencia de información y datos espaciales. Auditoría y certificación de repositorios digitales de confianza.* España: AENOR.

Asociación Española de Normalización y Certificación. (2018). *Norma UNE-ISO 23081-1:2018 Procesos de gestión de documentos Metadatos para la gestión de documentos. Información y documentación. Parte 1: Principios.* España: AENOR.

Barnard, A. (2011). *Archivos electrónicos: Textos y contextos.* Serie Formación Archivística. México: Archivo Universitario de la Universidad de Puebla.

Brown, A. (2008) *Digital Preservation Guidance 1. The National Archives.* Recuperado de: https://www.nationalarchives.gov.uk/documents/selecting-file-formats.pdf

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.

Ferreras, T. (2010). *Preservación digital en repositorios institucionales.* Salamanca: GREDOS.

InSPECT Project. (2008). *Significant properties*. Recuperado de http://www.significantproperties.org.uk/inspect-project/

Ivankovich, C. y Araya, Y. (2011). Focus groups: Técnica de investigación cualitativa en investigación de mercados. *Revista de Ciencias Económicas, 29*(1), 545-554. Recuperado de https://revistas.ucr.ac.cr/index.php/economicas/article/view/7057

National Library of Australia. (2003). D*irectrices para la preservación del Patrimonio digital de la UNESCO.* Recuperado de https://unesdoc.unesco.org/ark:/48223/pf0000130071_spa

OCLC y RLG. (2010). *Diccionario de datos Premis de metadatos de preservación versión 2.0.* Traduc. Lorea Elduayen y Bárbara Guiomar. Recuperado de: http://www.loc.gov/standards/premis/

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO). (s.f.) *SKOS: Tesauro de la UNESCO.* Recuperado de http://skos.um.es/unescothes/

Pauline, J. (2008). EDRMS 101: *The Basics. Information and Records Management Annual IRMA,* 25, 9-26. Recuperado de https://espace.curtin.edu.au/handle/20.500.11937/19879

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.

Térmens, M. (2013). *Preservación digital.* Barcelona: UOC.

Voutssas, J. y Barnard, A. (2014). *Glosario de Preservación Archivística Digital.* Versión 4.0. México: Instituto de Investigaciones Bibliotecológicas y de la Información, UNAM.

XXV Cumbre Iberoamericana de Jefes de Estado y de Gobierno. (2016) *Carta Iberoamericana de Gobierno Abierto.* Recuperado de: https://www.clad.org/images/declaraciones/CIGA-Octubre-2016.pdf