

ISSN: 0718 – 1701



UTEM

Serie Bibliotecología y Gestión de Información N° 43, Marzo 2009

**Directrices para la creación de un programa
de preservación digital**

Miguel Ángel Rivera Donoso



D · G · I

Departamento
de Gestión de
Información
Escuela de
Bibliotecología



Serie Bibliotecología y Gestión de Información es publicada desde Octubre de 2005 por el Departamento de Gestión de Información de la Universidad Tecnológica Metropolitana. Dr. Hernán Alessandri, 722, 6° piso, Providencia, Santiago, Chile, www.utem.cl

Sus artículos están disponibles en versión electrónica en E-prints in Library and Information Science: <http://eprints.rclis.org> y están indizados e integrados en la base de datos "Fuente Académica" de EBSCO Information Services.

Está registrada en el Sistema Regional de Información en Línea para Revistas Científicas de América Latina, El Caribe, España y Portugal (LATINDEX). Sitio Web: <http://www.bibliotecarios.cl/servicios/serie-bibliotecologia-y-gestion-de-informacion/>

Dirección Editorial

- Héctor Gómez Fuentes, Director (s) Departamento de Gestión de la Información
- Carmen Pérez Ormeño, Directora Escuela de Bibliotecología

Editor Jefe

- Héctor Gómez Fuentes

Consejo Editorial · Académicos del Departamento de Gestión de Información

- Mariela Ferrada Cubillos
- Cecilia Jaña Monsalve
- Guillermo Toro Araneda
- Alicia Ramírez González

Presidenta del Colegio de Bibliotecarios de Chile A. G.

- Paola Roncatti Galdames

Representante Legal

- Haydée Gutiérrez Vilches, Rectora (s)

Decano Facultad de Administración y Economía

- Enrique Maturana Lizardi

Secretaria del Departamento de Gestión de Información

- Carolina Osorio Silva

Diseño y Diagramación

- Programa de Comunicación y Cultura

Autorizada su reproducción con mención de la fuente.

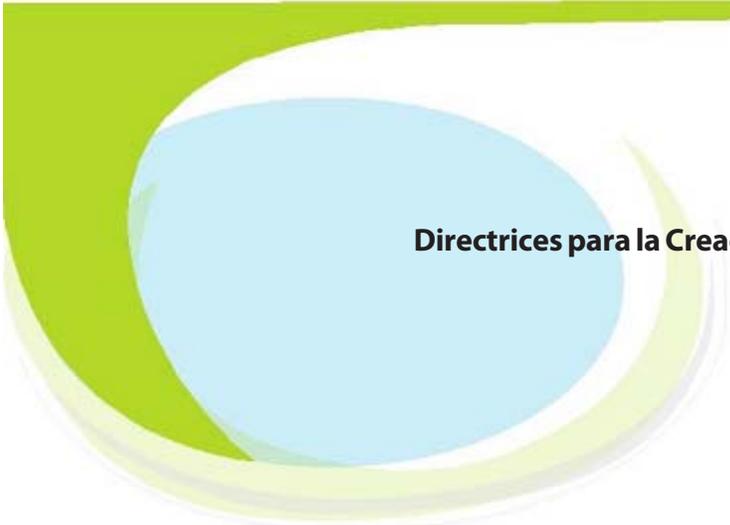
LAS IDEAS Y OPINIONES CONTENIDAS EN LOS TRABAJOS Y ARTÍCULOS SON DE RESPONSABILIDAD EXCLUSIVA DE LOS AUTORES Y NO EXPRESAN NECESARIAMENTE EL PUNTO DE VISTA DE LA UNIVERSIDAD TECNOLÓGICA METROPOLITANA.

TABLA DE CONTENIDO

Introducción	6
Acerca de este documento	8
1. La creación de un programa de preservación digital	10
1.1 Infraestructura de organización	10
1.2 Infraestructura tecnológica	12
1.3 Esquema de recursos	13
1.4 Modelo de referencia OAIS	13
2. Lo que amenaza a las colecciones digitales	16
2.1 Amenazas físicas	16
2.2 Obsolescencia	17
2.2.1 Obsolescencia de aplicaciones y archivos informáticos	17
2.2.1.1 Sugerencias para evitar la obsolescencia de archivos	18
2.2.2 Obsolescencia de equipos y hardware	19
2.2.2.1 Sugerencias para evitar la obsolescencia de equipos y hardware	19
3. Estrategias de preservación digital	20
3.1 Respaldo	20
3.2 Renovación del soporte de almacenamiento	21
3.3 Respaldo análogo	21
3.4 Replicación	22
3.5 Utilización de medios persistentes	23
3.6 Preservación de la tecnología	23
3.7 Mantenimiento físico de los equipos	24
3.8 Arqueología digital	25
3.9 Migración	25
3.10 Confianza en los estándares	27
3.11 Normalización	28
3.12 Emulación	29
3.13 Encapsulación	31
3.14 Computador virtual universal (UVC)	33
3.15 Canonicalización	35
3.16 Control de la autenticidad	35
3.17 Control de la estabilidad o integridad	36
3.18 Metadatos de preservación	38
4. Medios de almacenamiento y sus cuidados	42
4.1 Soportes magnéticos	42
4.1.1 Problemas que afectan a los soportes magnéticos	45



4.1.2 Sugerencias para la conservación de los soportes magnéticos	46
4.2 Soportes ópticos	46
4.2.1 Problemas que afectan a los soportes ópticos	48
4.2.2 Sugerencias para la conservación de los soportes ópticos	48
5. Cuestiones legales	50
5.1 Derecho de autor	51
5.2 En que afectan las cuestiones legales a la preservación	52
5.3 Sugerencias para abordar las cuestiones legales	55
6. Buenas prácticas y sitios Web relacionados	57
Bibliografía	59



Directrices para la Creación de un Programa de Preservación Digital*

Miguel Ángel Rivera Donoso

Master en Documentación Audiovisual

miguelrido@gmail.com

Resumen

Guía destinada a instituciones que inician el proceso de digitalización de sus documentos. Presenta requerimientos, problemas y estrategias a seguir para la preservación digital. Ofrece una amplia bibliografía de apoyo.

Palabras Claves:

<Conservación de documentos><Bibliotecas digitales><Preservación digital>

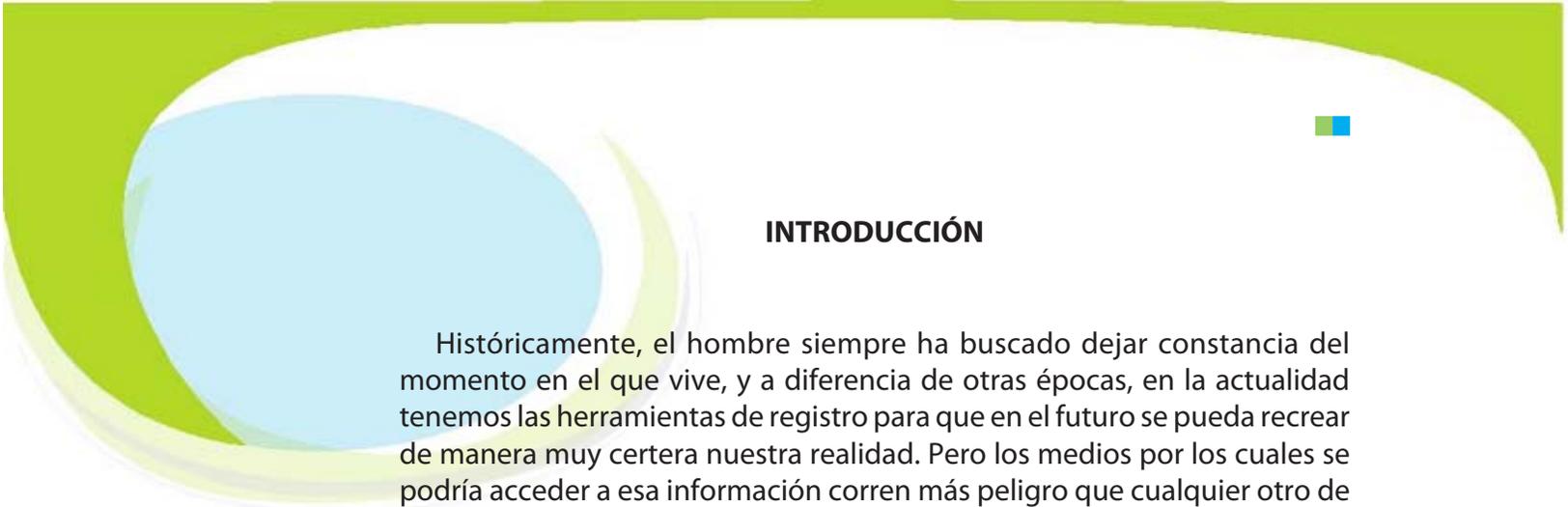
Abstract:

Guide aimed at organizations planning to digitize their documents. It outlines requirements, challenges and strategies for digital preservation. It provides an extensive bibliography on the subject.

Keywords:

<Documents Preservation> <Digital Libraries> <Digital Preservation>
<Preservation>

* Basado en la tesina para obtener el grado de Master en Documentación Audiovisual, Universidad Carlos III, Madrid, España.



INTRODUCCIÓN

Históricamente, el hombre siempre ha buscado dejar constancia del momento en el que vive, y a diferencia de otras épocas, en la actualidad tenemos las herramientas de registro para que en el futuro se pueda recrear de manera muy certera nuestra realidad. Pero los medios por los cuales se podría acceder a esa información corren más peligro que cualquier otro de la historia. Al menos hasta ahora, la información en soporte digital es más vulnerable que la película, que el microfilm, que el papel e incluso que los antiguos pergaminos y papiros.

Esto es debido a que estamos en unos momentos en el que las tecnologías digitales están avanzando velozmente, mejorando día a día sus posibilidades de publicación, edición, acceso, etc., por lo que en periodos muy cortos los formatos de escritura y lectura se modifican, dejando obsoletos a los anteriores. A esto se suma que la mayoría de las tecnologías están en manos de empresas privadas que pelean su hegemonía en el mercado, provocando serios problemas de compatibilidad entre ellas. Por otra parte, la transmisión de contenidos está fuertemente vigilada por legislaciones que protegen la autoría, limitando la distribución de los contenidos.

Todo esto provoca que la vida de los documentos digitales sea corta si estos se mantienen en su estado original, sin adecuarse a los cambios necesarios para poder subsistir.

Sin embargo, toda esta realidad se contrapone con el hecho de que el formato electrónico, por sus innumerables ventajas, se ha masificado tanto, que postula a convertirse en el único medio de escritura, registro y publicación de conocimientos y en general, de gran parte de la expresión humana. Muy pronto no se utilizarán cuadernos en los colegios, las publicaciones en papel paulatinamente desaparecerán, los antiguos sistemas de transmisión de TV o radio también, etc.

La información digital puede aparecer de dos maneras: digitalización de material análogo o información que se crea ya en entorno digital. En el primer caso, los problemas de conservación están relativamente solucionados a mediano plazo, puesto que se puede conservar el material original, más aún si desde el momento de la digitalización, toda la explotación del documento se llevará a cabo mediante la versión digital. Pero esto durará solo algunas décadas, pronto ya se habrá digitalizado todo, los escáneres se guardarán y nos encontraremos frente a un mundo de información íntegramente digital,



que a diferencia de aquella que se encuentra en los antiguos formatos, no se degrada paulatinamente, sino que puede desaparecer de un momento a otro.

Hay que preservarla, y hay que hacerlo ahora.

Aunque esta cuestión parezca nueva, los problemas que hicieron que se comenzara a hablar de preservación digital surgieron casi en conjunto con los primeros usos institucionales de este tipo de documentos. Sin embargo en la mayoría de los lugares las medidas no se tomaron o se procedió de manera inadecuada. Son incontables los ejemplos de información relevante que se perdió.

Tan solo en la segunda mitad de la década de 1990 se comenzó a hablar seriamente del asunto, hubo algunos estudios pioneros que alertaron a las instituciones más grandes, principalmente en los países anglosajones.

Recién en 2003, varias décadas después de la creación del mundo digital, UNESCO publica la Carta para la Preservación del Patrimonio Digital, referencia obligatoria para cualquier estudio del tema. La carta es un llamado a los estados y a las instituciones que custodian material digital para asumir la responsabilidad que significa el mantenimiento de la información que allí se encuentra.

El problema en absoluto es simple, los métodos aún no están acabados y quizás falte mucho para eso, ya que se necesita consenso entre muchas áreas; la preservación digital no sólo involucra a la documentación, sino que también a la ciencia, la informática, la economía y al mundo legal, como veremos detalladamente en este estudio.

De aquí en adelante, este problema atañe a todas las instituciones encargadas de custodiar información, de cualquier índole que esta sea, puesto que aunque no guarden material digital, tarde o temprano tendrán que digitalizarlo para cuidar tanto del original como del acceso a este.

Y en un futuro no muy lejano, este problema también nos afectará a modo individual; nuestros computadores cada vez necesitan más capacidad para almacenar las crecientes carpetas de fotografías o gigas de música y video. Al igual que las instituciones, tendremos que organizarnos para no perder nuestra información, que es parte de nuestra memoria, tanto individual como colectiva.





Acerca de este documento

Hasta el momento es muy poco el material de estudio sobre preservación digital que se puede encontrar en español, esto debido a que es una problemática asumida hace muy pocos años y los principales exponentes aún son solamente los países anglosajones más Holanda, que también ha aportado interesantes investigaciones. No obstante, los formatos digitales ya están presentes en casi todo el mundo y por lo tanto las necesidades de preservación también.

El siguiente estudio está pensado para que sea utilizado como herramienta por las instituciones que no han iniciado el proceso de digitalización de sus documentos, o por aquellas que lo han comenzado hace muy poco y pretenden que sus nuevos formatos sean preservados a mediano y largo plazo.

El documento abarca las diferentes áreas que se deben considerar para montar un programa de preservación con bases suficientes que permitan que este no tropiece en el camino.

Como fuente para este estudio se ha utilizado una amplia bibliografía que se detalla al final, sin embargo algunos documentos son las bases y los pilares fundamentales, puesto que son los más desarrollados y que han servido de referencia para la mayoría de los programas de preservación digital que ya están en curso.

Estos documentos son los siguientes:

- *Digital Preservation Management: Implementing short-terms strategies for long-term problems*. Cornell University Library. (2004-2007)
http://www.icpsr.umich.edu/dpm/dpm-eng/eng_index.html
- *Preserving Access to Digital Information (PADI)*. National Library of Australia (2001-2007)
<http://www.nla.gov.au/padi/>
- *Directrices para la Preservación del Patrimonio Digital*. UNESCO, prepared by the National Library of Australia. (2003)
http://www.imaginar.org/dppd/DPPD/0_DPPD.pdf (Traducido al español)
<http://unesdoc.unesco.org/images/0013/001300/130071e.pdf> (Original en inglés)



- *Preservation Management of Digital Materials: A Handbook*. Jones, Maggie, and Neil Beagrie. (2001)
<http://www.dpconline.org/graphics/handbook/index.html>
- *Reference Model for an Open Archival Information System (OAIS), Blue Book*. (2002)
<http://public.ccsds.org/publications/archive/650x0b1.pdf>
- LIBRO "La preservación de recursos digitales, El reto para las bibliotecas del siglo XXI" Alice Keefer, Núria Gallart.

1. La creación de un programa de preservación digital

Como explicábamos anteriormente, las preocupaciones reales por la preservación digital comenzaron a concretarse tan solo a mediados de la década de 1990.

Uno de los estudios pioneros, *Preserving Digital Information: Final Report and Recommendations*, publicado en 1996, se refiere a la necesidad de crear centros especializados para preservar contenidos digitales.

<http://www.oclc.org/programs/ourwork/past/digpresstudy/default.htm>

En esos momentos, por falta de experiencia o por la magnitud de los requerimientos, no fue posible crearlos, pero actualmente el asunto se ha asumido con verdadera responsabilidad y, principalmente en los países más desarrollados económicamente, se han llevado a cabo interesantes programas de preservación.

Lamentablemente los requisitos para montar un programa en óptimas condiciones siguen estando fuera del alcance de la mayoría de las instituciones. Sin embargo, las experiencias han derivado también en esfuerzos para mostrar el camino y dar las claves para que un programa que se inicia, no parta desde el total desconocimiento.

En esta sección entregamos algunos consejos básicos, que se constituyen como un buen punto de partida.

Los estudios de la Universidad de Cornell sostienen que un programa de preservación digital se debe edificar sobre tres grandes pilares inseparables que merecen una atención constante. Estos son:

- Organización
- Tecnología
- Recursos económicos

1.1 Infraestructura de organización

Se refiere a los procedimientos y políticas organizativas que la institución adopta para llevar a cabo el programa.

Se ha dicho en reiteradas ocasiones que un organismo que asuma la responsabilidad de preservar contenido digital, debería tener la misma fiabilidad que ahora tienen los museos o las bibliotecas nacionales con



respecto a la autenticidad e integridad de sus colecciones, esto debido a la facilidad con que un objeto digital puede ser modificado.

Además de mantener esta fiabilidad en el tiempo, pese a los cambios de la tecnología y del mercado, una institución de este tipo debe contar con las herramientas para identificar y recuperar la información, establecer políticas de acceso razonables, tener una tecnología idónea para la preservación, cuidar de los derechos intelectuales y asegurar que los metadatos sean normalizados y estén siempre vinculados a la información. También las metodologías propuestas por el programa de preservación deben contar con el acuerdo de las partes involucradas en el proyecto, que pueden ser creadores, distribuidores, gestores, financistas y usuarios.

Una institución que decide preservar, debe estar siempre actualizada de lo que el mundo tecnológico propone, a la vez que estar al corriente de las buenas prácticas que otras instituciones van adoptando. Hasta que se creen parámetros globales comunes para la preservación digital, la estrategia de la colaboración es fundamental.

La Universidad de Cornell propone algunos consejos al respecto:

- Suscribirse a padiform-I, que es una lista de publicaciones e intercambio de ideas para la preservación digital, coordinado por la Biblioteca Nacional de Australia.
<http://www.nla.gov.au/padi/forum/>
- Suscribirse a IFLA DIGLIB una lista activa sobre información de bibliotecas digitales, con un buen número de noticias sobre la preservación y tecnologías digitales.
<http://infoserv.inist.fr/wwsympa.fcgi/info/diglib>
- leer DIGINEWS (descontinuado desde 2007, aunque sus archivos están disponibles y se encuentran artículos muy interesantes).
<http://www.oclc.org/programs/publications/newsletters/diginews.htm>
- y D-LIB magazine
<http://www.dlib.org/>

Es muy probable que la creación de un departamento o área de preservación digital, lleve consigo una serie de cambios que pueden no ser muy bienvenidos, como cambio de personal, de locaciones, de procedimientos, aumento de responsabilidades, etc.



1.2 Infraestructura tecnológica

Consiste en el equipamiento indispensable para almacenar, conservar y poner a disposición la información para el usuario, esto incluye hardware, software, el espacio físico, las condiciones de control del ambiente y el personal que trabajará. Cada uno de estos merece una atención especial antes de montar el programa, para que sobre la marcha no aparezcan sorpresas que escapen a las condiciones iniciales.

Por ejemplo, los equipos necesarios son muchos más que los dispositivos de captura y almacenamiento de la información. Las necesidades van desde los servidores y los medios de almacenaje "en línea", hasta detalles como la amplitud de los escritorios, la cantidad de tomas de corriente o los carros móviles para trasladar los medios.

El tema del almacenamiento merece una especial atención, puesto que es muy probable que en poco tiempo el volumen de información aumente considerablemente, y como se detallará en las estrategias de preservación, es indispensable tener más de una copia.

Es cierto que los medios de almacenamiento cada vez entregan más capacidad y velocidad de acceso, así como también disminuyen sus costes; sin embargo la capacidad del depósito continúa siendo uno de los principales problemas.

De ser posible, es recomendable tener un depósito "en línea", tal como un sistema RAID. Pero pese a la velocidad de acceso que entrega este sistema, es un tipo de almacenamiento relativamente costoso y vulnerable a pérdida, por lo que también se recomienda utilizar almacenamiento "nearline", que significa almacenamiento seguro en disco o cinta, pero con recuperación automatizada.

Todo esto complementado con CDs y DVDs que se irán "refrescando" periódicamente.

Por otra parte, es indispensable no descuidar de las aplicaciones informáticas que gestionarán la colección. El software de depósito merece una atención especial, pues es el que otorgará las posibilidades de almacenamiento, manejo y entrega de los materiales. Hasta el momento se han desarrollado muchas aplicaciones para estos efectos, tanto de propietarios como abiertos. Cada institución debe optar por el que mejor se adapte a sus necesidades específicas.



A continuación se citan tres ejemplos que han tenido buena aceptación en la comunidad de archivos digitales:

FEDORA <http://www.fedora-commons.org/>

DSPACE <http://www.dspace.org/>

GREENSTONE <http://www.greenstone.org/>

1.3 Esquema de recursos

Se trata de todos los requerimientos económicos que la institución tiene que prever antes de comenzar el proyecto.

Se debe contemplar que un programa de preservación requiere una inversión constante, no basta tan solo con un gran monto al comienzo. Ya que se necesita periódicamente ir renovando los abundantes soportes y equipos, pagar los salarios del personal, que en condiciones ideales deberían ser varias personas; financiar los planes de emergencia, la adquisición de derechos y licencias, etc.

Algunas instituciones, debido a su experiencia, aconsejan que si no se cuenta con los fondos económicos necesarios, es mejor esperar a que exista la seguridad de que estos estarán, puesto que a la larga, puede resultar incluso más costoso retomar un proyecto que se había abandonado por falta de recursos.

La Universidad de Cornell ha preparado un test para saber si están las condiciones para afrontar un plan de preservación.

<http://www.icpsr.umich.edu/dpm/dpm-eng/foundation/tdr/readiness.pdf>

1.4 Modelo de Referencia OAIS (Open Archive Information System)

El modelo OAIS fue creado originalmente por la NASA para gestionar su vasto material digital y en el año 2002 adoptado por la unión de dos grandes consorcios de bibliotecas norteamericanas: RLG y OCLC, para convertirse en el modelo de referencia de cómo debe comportarse una institución que asuma la responsabilidad de preservar contenidos digitales a largo plazo.

Hasta el momento, esta iniciativa es la más completa y la más adoptada por los grandes programas de preservación digital.

OAIS estandariza la manera de gestionar los materiales que preservará, desde el ingreso hasta la publicación y puesta a disposición del público.



Este modelo no es el diseño concreto de un programa, sino que dicta una serie de pistas, que luego cada institución deberá readecuar a su realidad y a sus necesidades, por ejemplo, en relación a las cuestiones de acceso.

OAIS propone seis pasos ineludibles para un programa, cuatro de ellos son actividades a las que se somete el material almacenado:

- Incorporación (ingest)
- Almacenamiento (archival storage)
- Gestión (data Management)
- Acceso/difusión (access/dissemination)

Y dos hablan del funcionamiento del depósito

- Planificación para la preservación (preservation planning)
- Gestión del depósito (archive administration)

Una propuesta fundamental es la normalización de la terminología relacionada con un programa de preservación, un paso clave que favorecerá la interoperabilidad en el futuro.

Dentro de esta terminología propuesta, está el **paquete de información IP** (Information Package) que se refiere al conjunto que conforma el objeto digital con sus metadatos.

El IP tiene tres versiones según su estado:

- **SIP** (Submission Information Package), que es el paquete cuando entra al depósito.
- **AIP** (Archival Information Package) que es cuando el IP ya tiene las modificaciones necesarias para ser almacenado en bitstream o cadena de bit.
- **DIP** (Dissemination Information Package), que es el recurso listo para ser puesto a disposición de los usuarios.

En el DIP, posiblemente la información estará muy cambiada a como entró en el SIP, pues puede tener nuevos metadatos o haber sufrido migraciones. Cuando los materiales ingresan al programa, se deben tomar ciertas medidas de reconocimiento, como el formato, las especificaciones de este, ver si dentro de este formato hay otros involucrados, etc. También el modelo propone que si el ingreso lo hace otra institución, esta debe tener las

responsabilidades de preparar el material para que tenga las condiciones propuestas.

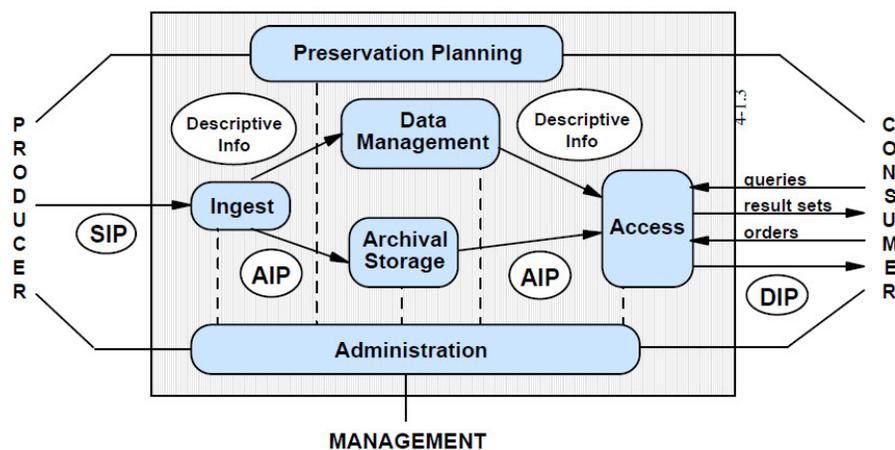


Figura 1: Gráfico de funcionamiento de las entidades de OAIS

Existe una versión interactiva de este gráfico y con la explicación de cada una de sus partes en:

<http://www.icpsr.umich.edu/dpm/dpm-eng/terminology/full.html#archival>

El Modelo de Referencia OAIS:

<http://public.ccsds.org/publications/archive/650x0b1.pdf>

Tutorial OAIS (PowerPoint)

[OAIS Tutorial, 2002-10-25 \[PPT\] \(269,312 bytes\)](#)

2. Lo que amenaza a las colecciones digitales

Tenemos asumido que la durabilidad del objeto digital aún no se puede medir. Ni siquiera podemos aproximarnos, como sucede con los objetos tradicionales, que se degradan lentamente y en muchos casos podemos calcular las expectativas de vida de acuerdo al tipo de material y a la experiencia que hemos tenido con él en el pasado.

Con pocas décadas de existencia, el documento digital ha demostrado ser mucho más frágil desde el punto de vista de la conservación, pues en ella hay involucrado una serie de factores impensables en los documentos no digitales, como la dependencia de un equipo que interprete el contenido, la rápida renovación de los soportes de almacenamiento y lectura que dejan obsoletos a los anteriores, las infinitas modificaciones que se pueden ir sumando en el mismo documento, etc.

Nada puede asegurar, como sucede con el papel por ejemplo, que un archivo digital esté disponible en cinco o diez años más, puesto que para ello se necesita una inversión continua, lo que escasea en la gran mayoría de las instituciones culturales, y aunque esa inversión fuese la ideal, estas instituciones están sujetas a los cambios y a los intereses de la industria, lo que no se puede predecir. Por tanto, los programas de preservación tienen que mantenerse a base de especulaciones.

Lo más lamentable de todo, no es la pérdida del objeto mismo, pues en el mundo digital el continente no tiene en absoluto un valor equivalente al contenido, como muchas veces sucede con los materiales tradicionales. Más bien, el objetivo final de la preservación digital, es el mantenimiento de la información misma. Desde hace décadas existen muchas investigaciones, creaciones o expresiones varias que solamente se encuentran en formato digital, y si este se pierde, la pérdida de ese contenido puede ser irremediable. Esto ocurre tanto en lo institucional como en lo doméstico.

Descontando las cuestiones legales y económicas, los contenidos almacenados digitalmente se pueden perder de dos maneras: daño físico y obsolescencia.

2.1 Amenazas físicas

Pueden suceder en cualquier momento por razones internas o externas y afectar a todos los materiales indispensables para acceder al contenido digital.



El deterioro físico puede ser causado por factores mecánicos, químicos y biológicos.

Los daños ocurren de diversas maneras:

- Desastre natural (incendio, terremoto, tormenta, etc.)
- Condiciones inadecuadas de almacenaje, como temperaturas y porcentajes de humedad relativa extremos o bien, inestables. Esta es la principal razón de desgaste prematuro de los equipos.
- Fallos de energía
- Mal mantenimiento de los equipos de hardware.
- Abuso en la utilización de los mecanismos manuales.
- Fallos humanos, como la incorrecta manipulación de los medios, el derramamiento de líquidos, caídas de equipos, etc.
- Actos malintencionados, como robos, virus, sabotajes, etc.
- Deterioro natural de los equipos.

Factores como los desastres naturales o los actos malintencionados no se pueden predecir, pero sí se puede hacer todo lo posible, tanto para prevenirlos como para montar un plan de emergencia.

2.2 Obsolescencia

La amenaza de pérdida por obsolescencia es aún más grave que la de deterioro físico, puesto que es más difícil de controlar al haber más factores involucrados.

Diferenciaremos entre dos tipos de obsolescencia:

- Aplicaciones y archivos informáticos
- Equipos y hardware

2.2.1 Obsolescencia de aplicaciones y archivos informáticos

Hasta la fecha se han creado miles de formatos, y antes de la década de los 90 no se hizo casi ningún esfuerzo por conservar o documentar sus especificaciones, lo que ha producido la pérdida, sin remedio hasta el momento, de incontable información relevante. Desde hace muy poco tiempo han comenzado a multiplicarse los esfuerzos para identificar e interpretar archivos antiguos, pero es una ardua tarea.

Normalmente una nueva versión de software puede leer sus archivos anteriores, pero esto rara vez supera las tres generaciones hacia atrás, por lo que los ficheros más antiguos quedan irrecuperables y la versión de la aplicación que podía leerlos, ya no está disponible o no es legible por los nuevos equipos.



El mayor riesgo lo constituyen los “formatos propietario” cuya especificación no está disponible públicamente, por lo que pueden ser interpretados tan solo por el software de la misma empresa, y si esta decide cambiar el formato o discontinuar el software, o bien cae en la quiebra o se fusiona con otra, los archivos dependientes de ella podrían quedar ilegibles. Esto ya ha sucedido.

Contrario a esto son los formatos con especificaciones abiertas, generados ya sea por compañías privadas (Adobe PDF, TIFF o SWF) o por organizaciones que fomentan el uso de los estándares abiertos (JPG, XML, SVG, MPEG-2).

Los estándares abiertos tienen una buena compatibilidad hacia atrás, pues no intentan dejar obsoletos los formatos por razones comerciales. Más detalles de este tema en “Confianza en los estándares” (Pág. 29)

Sin embargo, hasta el momento las aplicaciones y archivos más exitosos y duraderos, son los “formatos propietario”.

Resumiendo, los motivos por los que un archivo podría quedar obsoleto son los siguientes:

- El software que lo lee es discontinuado.
- Un software moderno no lee sus formatos antiguos.
- Un formato se hace más complejo o es reemplazado.
- El formato no es lo suficientemente masivo, por lo que desaparecen las aplicaciones compatibles.

2.2.1.1 Sugerencias para evitar la obsolescencia de archivos

- En el orden de las actividades de preservación, se deben privilegiar los objetos creados con aplicaciones obsoletas o con peligro de obsolescencia. Por supuesto, examinando previamente si el contenido de estos documentos merece el esfuerzo.
- Para la elección de los formatos, se debe optar por aquellos que tengan más inmunidad a la obsolescencia, por ejemplo:
 - Que tengan buena compatibilidad hacia atrás.
 - Que sean ampliamente utilizados globalmente.
 - Que no sean excesivamente complejos ni tampoco demasiado simples.
 - Que tenga chequeo de errores incorporado.
 - Que tengan un ciclo de actualizaciones relativamente frecuente.
 - De preferencia, que sean formatos abiertos.



2.2.2 Obsolescencia de equipos y hardware

La amenaza de obsolescencia de los equipos no es tan sólo para aquellos que pertenecen al entorno informático, sino que también para los de cualquier otro tipo de tecnología. Desde hace siglos es un problema que afecta a los consumidores y habitualmente beneficia a la industria. Lamentablemente, en las últimas décadas muchos equipos están diseñados para tener un periodo de vida útil relativamente corto. Es posible que los fabricantes tengan las tecnologías para confeccionar equipos de larga duración, por ejemplo, con amplia capacidad de memoria o buena resolución de video, pero sin embargo los van introduciendo poco a poco en el mercado, para así favorecer la obsolescencia y por supuesto, sus beneficios económicos.

En el caso de los equipos informáticos, cada vez con mayor frecuencia, las maquinas van siendo reemplazadas por otras nuevas más efectivas en cuanto a capacidad, velocidad, energía, eficacia, etc.

También las nuevas versiones de software, que generalmente otorgan posibilidades más amplias, van exigiendo mayor efectividad de hardware. Lo que provoca que ambos crecimientos y obsolescencias sean proporcionales.

Además, junto con la renovación de las tecnologías internas de los equipos, van cambiando también las tecnologías externas, como las conexiones periféricas (por ejemplo, la conexión firewire y los puertos USB han sustituido a tecnologías de conexión como RS-232 o los puertos paralelos Centronics) o los equipos externos, como pendrives, discos duros externos, escáneres e impresoras.

2.2.2.1 Sugerencias para evitar la obsolescencia de equipos y hardware

- Comprar medios de calidad, aunque esto resulte más costoso.
- No proyectar los equipos a más de cinco años de vida útil.
- No realizar compras exageradas, Puesto que en algunos años habrá que renovar y algunos equipos podrían quedar sin uso.
- Habitualmente visitar el sitio Web del fabricante para realizar un seguimiento del equipo o de la familia de estos, a la vez que actualizarse de las nuevas tecnologías
- Realizar pruebas periódicas para ver el estado de los datos.

La Universidad de Cornell ha desarrollado un sitio Web, llamado "La cámara de los horrores" en el que se enumeran y describen la mayor parte de los soportes que están obsoletos o en vías de obsolescencia.

<http://www.icpsr.umich.edu/dpm/dpm-eng/oldmedia/chamber.html>

3. Estrategias de preservación digital

En pocos años, la experiencia no es mucha para poder afirmar qué estrategias son las más apropiadas y efectivas para la preservación a largo plazo, no obstante, estos años sí han sido suficientes para poder asegurar que mientras antes se tomen las medidas, mejor.

Sabemos que ningún soporte de almacenamiento puede durar para siempre, por lo que hay que ir constantemente buscando las mejores opciones para mantener la legibilidad de los archivos.

Las instituciones han adoptado medidas diferentes de acuerdo a cada riesgo, pero al recopilar las prácticas asumidas en los principales centros, podemos ver que muchas coinciden.

Hasta la fecha, ninguna estrategia por si sola es capaz de solucionar el problema, aún estamos lejos de eso. Por el momento, la mejor práctica, es la mezcla de las estrategias propuestas. Confiamos en que en el futuro la tecnología nos entregue más herramientas para facilitar la tarea.

En los estudios que se han publicado, podemos ver que las estrategias cambian de nombre o se agrupan de distinta manera. Describiremos la mayor cantidad posible.

En esta unidad, algunas estrategias serán más desarrolladas que otras debido a su mayor envergadura, como es el caso de los metadatos, la migración o la emulación, entre otras.

3.1 Respaldo

Se trata simplemente de hacer un duplicado exacto del objeto que se intenta preservar. En cualquier programa de preservación digital, el respaldo debe ser considerado el recurso mínimo de mantenimiento, que debe abarcar a la totalidad de los archivos, incluso a aquellos que son considerados de bajo valor.

La duplicación es un componente esencial de la preservación puesto que se ocupa de la pérdida de datos por problemas de hardware u otros fallos como el mal funcionamiento de los equipos, el deterioro, desastres naturales, etc.

Sin embargo, al no hacer frente al problema de la obsolescencia, el respaldo tan solo es considerado una estrategia para el corto plazo.



El respaldo debe siempre ir acompañado de almacenamiento remoto, de esta manera se evita que un mismo desastre altere la totalidad de las copias.

3.2 Renovación del soporte de almacenamiento

También conocido como “refreshing” o “refresco” es, al igual que el respaldo, una estrategia para reducir el riesgo de pérdida debido al deterioro de los soportes, y que se basa en realizar una copia, sin alterar en absoluto la información digital, pero con la diferencia de que se buscan soportes de almacenamientos más modernos. Por ejemplo, el traspaso de datos desde un CD-RW antiguo a uno nuevo.

“Modified refreshing” es un traspaso similar, pero hacia un soporte nuevo con mayor capacidad de almacenamiento, por ejemplo la transferencia de datos desde una cinta QIC a una cinta DLT.

Estas restauraciones de los datos, además del deterioro, se ocupan de algunos problemas de obsolescencia, pero aún así no son suficientes para ser consideradas una estrategia completa de preservación, puesto que debe combinarse con otras técnicas que tratan también el problema de la obsolescencia del software. No obstante, en el corto plazo, es una excelente estrategia.

Para definir la frecuencia de tiempo con la que se debería realizar el refresco es conveniente considerar las recomendaciones de los fabricantes, pero también dependerá de la cantidad de uso y las condiciones de almacenamiento.

3.3 Respaldo análogo

Esta estrategia es el copiado de seguridad de la información digital en soportes no digitales. La historia de los soportes análogos aún es bastante más extensa que la de los digitales, y en esa historia algunos materiales han demostrado ser más duraderos que otros.

El almacenamiento análogo es muy bueno contra la obsolescencia, pero tiene problemas con la degradación de la calidad, puesto que el copiado o la transferencia conllevan pérdida. No obstante, los documentos de texto o de imágenes monocromáticas tienen una pérdida casi inapreciable, por lo que se benefician de esta estrategia.

Lamentablemente el costo de estos aparatos, o del servicio de almacenamiento mediante ellos, es todavía muy elevado, por lo que, si no se



cuenta con los medios económicos suficientes, es recomendable tan solo para aquellos documentos que deben ser preservados de todas maneras.

Actualmente varias empresas fabrican medios de almacenamiento análogo pensados en la preservación a largo plazo. Dos ejemplos importantes son el HD Rosetta de la empresa *Norsam Technologies*:

<http://www.norsam.com/hdrosetta.htm>

y los microfilm de haluros de plata de *Kodak*:

<http://graphics.kodak.com/docimaging/CL/es/Products/Micrographics/Microfilm/index.htm>

Un buen proyecto de demostración de conversión desde soporte digital hacia microfilm fue realizado por la Universidad de Cornell entre los años 1994 y 1996 y los resultados están publicados en:

<http://www.library.cornell.edu/preservation/com/comfin.html>

3.4 Replicación

Es el duplicado y el copiado de la información en uno o más sistemas y su principal fortaleza es el almacenamiento en más de un lugar para de esta manera evitar que una misma alteración, intencional o accidental, o el mismo desastre natural pueda hacer que se pierda la totalidad de la información.

Al igual que otras estrategias, la replicación también pretende la longevidad de la información mediante el copiado, el almacenamiento en distintos lugares y la actualización del ambiente tecnológico que la rodea, y por tanto tiene los mismos riesgos, ventajas y desventajas que estas otras estrategias.

En el fondo, la replicación es la suma de varias de las políticas de preservación que hemos descrito. OAIIS considera la replicación una manera de migración.

Es importante señalar que mientras más copias almacenadas existan, mucho mayor es el costo de la mantención, el respaldo y la actualización periódica que requiere todo el archivo, pero sin duda, como habíamos mencionado anteriormente, ningún programa de preservación digital puede considerarse como tal, si no tiene al menos un depósito físico remoto.

La replicación puede concebirse de diversas maneras. Por ejemplo como un programa de alguna institución que, entre otras estrategias, aplique el almacenamiento en diversos lugares.



Un interesante programa de este tipo es LOCKSS (Lots of Copies Keep Staff Safe) de la Universidad de Stanford: <http://www.lockss.org/lockss/Home> y su variante CLOCKSS (Controlled LOCKSS) que se especializa en la preservación a largo plazo.

Pero otra manera distinta de replicación puede ser una red informática Peer-to-peer (P2P). <http://es.wikipedia.org/wiki/Peer-to-peer>

Un sitio con interesante información al respecto:
http://www2.ub.edu/bid/consulta_articulos.php?fichero=20casti2.htm

3.5 Utilización de medios persistentes

Se trata de la utilización de medios más resistentes y perdurables. Ayuda de esta manera a reducir las pérdidas que se deben al deterioro de los medios de almacenamiento comunes, ante los cuales hay que tener especial cuidado en su manipulación, control de la humedad y temperatura, almacenamiento, etc. Por otra parte, si se implementa esta estrategia, no es necesario realizar el "refresco" tan frecuentemente.

Ejemplos de soportes persistentes son los CDs o DVDs de platino o de oro. Sin embargo no podemos confiar ciegamente en esto, puesto que nada puede hacer frente a amenazas tales como la obsolescencia de los medios de codificación o los desastres naturales o malintencionados.

3.6 Preservación de la tecnología

Consiste en la conservación de todo el entorno técnico que tiene relación con una colección digital.

Entre estas prácticas, se encuentran la mantención de los sistemas operativos, del hardware y de la aplicación original del software.

Todas estas medidas están pensadas para hacer frente a la obsolescencia de los medios y recuperar la legibilidad de los archivos ante los cuales no se aplicaron políticas adecuadas de preservación.

Por ejemplo, muchas instituciones continúan conservando computadores que siguen trabajando con un programa específico que funciona en un entorno MS-DOS.

Pero esta estrategia de ninguna manera podría ser considerada para largo plazo, debido a que las cualidades de hardware y software continúan



creciendo en complejidad, además muchas piezas para hardware dejarán de ser proveídas por los fabricantes. Por otra parte, el desgaste químico y físico propio de los aparatos y sus componentes en algún momento harán imposible su mantenimiento. Finalmente, la implementación de esta tecnología requiere un gasto económico y humano muy grande, que muchas instituciones no podrían llevar a cabo, al menos de manera individual.

3.7 Mantenimiento físico de los equipos

Intenta evitar la pérdida de los dispositivos por motivos de deterioro, de manera que esto no afecte en el corto plazo las estrategias pensadas a largo plazo.

Como hemos descrito en la sección “Amenazas físicas” hay una serie de factores que atentan contra la integridad de los equipos y que muchas veces no se pueden predecir, sin embargo se pueden reducir al mínimo los riesgos. Las sugerencias de conservación, detalladas por tipo de soporte, se encuentran a partir de la página 42, pero a continuación enumeramos las más elementales y que son comunes para todos los dispositivos:

- Mantener estables las condiciones de temperatura y humedad.
- Controlar el polvo y los vapores.
- Tener equipos de detección de fuego, humo, temperaturas extremas y escapes de agua.
- Acceso restringido a los almacenes.
- Prohibir comer, beber y fumar en las dependencias donde se encuentren los medios.
- Para la manipulación, tener las manos siempre limpias y secas.
- No apilar los soportes.

<http://www.climatenotebook.org/MSQR/MSQR.pdf> (breve manual de almacenamiento de los medios).

3.8 Arqueología digital

Se trata de una estrategia de emergencia que intenta rescatar los contenidos digitales que estaban almacenados en medios que han sido dañados físicamente, o que pertenecían a entornos de hardware y software obsoletos o dañados.

Para llevar a cabo esta estrategia, es necesario aplicar técnicas especializadas para recuperar la información que aunque sigue estando almacenada, no puede ser interpretada por los medios y por tanto, se ha convertido en ilegible.



Ejemplo de estos fallos son los desplomes de discos, o cintas que se han arrugado.

Aunque muchos soportes tienen daños que hacen irrecuperable la información, también es posible rescatar otros que aparentemente están perdidos, pero los costes que significa esta recuperación suelen ser aún muy elevados.

Últimamente se han creado muchas empresas de recuperación de datos desde soportes dañados, una simple búsqueda en Internet arroja muchos resultados.

No se debe confundir esta estrategia con la Arqueología Digital como disciplina de búsqueda de contenidos antiguos en la Web, sobre todo porque esta última actualmente tiene mucha más cobertura mediante blogs o páginas especializadas.

3.9 Migración

La migración es una estrategia un poco más compleja que las anteriores y es una de las más consideradas dentro de los planes de preservación digital. Sabemos bien que la información digital es inútil si no está codificada para que pueda ser legible por personas, por lo tanto el principal objetivo de la migración es conseguir la mantención de la accesibilidad a los recursos digitales para que cualquier usuario, en cualquier momento, pueda recuperarla sin que los cambios tecnológicos la alteren, o al menos no demasiado.

Esta estrategia se compone de una serie de tareas organizadas y diseñadas para lograr la transferencia periódica de información digital desde un sistema a otro más reciente, más seguro o que entregue mejores posibilidades. Esta transferencia puede ser desde un formato a otro (por ejemplo desde un documento de Microsoft Word a uno de PDF), desde un sistema operativo a otro (por ejemplo desde Windows a Linux) o desde un lenguaje de programación a otro (por ejemplo desde BASIC a JAVA) así se intenta asegurar por un tiempo más la accesibilidad al objeto digital.

En líneas generales, la migración ocupa la renovación de soportes de almacenamiento (refreshing), sin embargo no siempre es posible hacer una copia exacta de un objeto digital pues algunos cambios de hardware o de software dejan irreconocibles algunas tecnologías anteriores.



La migración va más allá de la intención de evitar el deterioro físico, sino que hace frente también a la obsolescencia de la codificación de datos y para esto busca siempre la mejor opción para continuar visualizando el objeto, y si se quiere, alterándolo, con el mayor número de posibilidades que en esos momentos nos entregue la tecnología.

De la migración se han beneficiado de muy buena manera hasta el momento los documentos de texto, hojas de cálculo, imágenes y video, entre otros.

Pero pese a parecer una muy buena estrategia, hasta el momento tiene una serie de problemas y riesgos:

- Aún no ha sido totalmente comprobada, sobre todo con elementos más complejos como páginas Web o algunas bases de datos.
- No siempre se cuenta con los datos de las codificaciones anteriores, sobre todo en los formatos cerrados o de propietario; este problema se agranda con la necesidad de sucesivas migraciones.
- Como no siempre es posible hacer copias exactas, sobre todo cuando se transfiere desde una tecnología anterior a una subsecuente, se trata de interferir lo menos posible, pero tras la acumulación de varias migraciones estos cambios pueden acrecentar demasiado las diferencias con el material original.
- Los nuevos formatos pueden ser incapaces de interpretar toda la funcionalidad del formato original.
- Normalmente las empresas proporcionan compatibilidad con sus productos de software anteriores, pero esto rara vez sobrepasa tres generaciones, por lo que las versiones anteriores a estas pierden la compatibilidad o bien la conservan con pérdidas.
- No es un plan de preservación por si mismo, puesto que está aún lejos de resolver los problemas de la mantención de la integridad, apariencia y autenticidad de los contenidos digitales.
- Los costos para migrar todo un archivo pueden llegar a ser muy altos, por lo que muchas instituciones han tenido que privilegiar unos contenidos por sobre otros, lo que genera un grave riesgo de pérdida irreparable para mucha información.

No obstante, las técnicas para mejorar la migración se siguen desarrollando para resolver estos problemas y así afianzar esta estrategia que, en opinión de muchos, es la que otorga mejores posibilidades para conservar material digital a largo plazo.

3.10 Confianza en los estándares

Significa la utilización de los estándares más corrientes, depositando toda la confianza en que la industria siempre proporcionará productos que sean compatibles con sus anteriores formatos y con el entorno computacional común. La idea principal de esta estrategia es favorecer los estándares más conocidos, intentando dejar en el olvido aquellos más nuevos o con menos fundamentos. Se supone que los sistemas operativos y las aplicaciones se adaptarán a estos estándares.

La confianza en los estándares puede bloquear las amenazas de obsolescencia a corto plazo para los documentos digitales, pero la mayor parte de la industria se ha caracterizado en no considerar demasiado los problemas de preservación digital, por lo que nos puede sorprender en cualquier momento, como ha sucedido en anteriores ocasiones, ocultando la especificación de sus formatos o simplemente, eliminándolos del mercado. Vale mencionar que dentro de los formatos estándares existen los formatos abiertos y los formatos propietario o privados. Abiertos son aquellos que han dejado en el dominio público las especificaciones (código fuente) para que un software pueda interpretar la codificación del bitstream, por lo que se pueden crear aplicaciones que no pertenezcan a la misma compañía y que interpreten el documento para que este sea legible. Por el contrario, muchas empresas, por razones comerciales, guardan las especificaciones de sus formatos en secreto para que sólo puedan ser interpretadas por sus propios programas o bien para venderlas, siempre bajo cláusula de no publicación de ella; estos son los formatos propietario. También existen estándares semilibres, que pueden ser de compañías privadas, pero que han dejado las especificaciones disponibles.

Es de suponer que para la preservación digital se recomienda utilizar siempre estándares abiertos, para que la legibilidad de los documentos no esté condicionada por el devenir de la compañía fabricante del software o archivo ni por la incertidumbre acerca de cuestiones legales que puedan ocurrir más adelante.

El objetivo principal de los estándares abiertos es que se pueda crear la competencia entre diversos tipos de programas o archivos para así mejorar la calidad, a la vez que impedir que el vendedor ejerza el control sobre el futuro de la información. Por otra parte, permite la compatibilidad y por lo tanto, la interoperabilidad entre los distintos programas. Cabe señalar que los formatos de archivo abiertos normalmente pueden ser leídos por aplicaciones informáticas libres o abiertas, que también son creados por un mercado libre, lo que reduce los gastos para muchas instituciones que deben pagar las licencias y los sobrecargos de los programas comerciales.



Por todo esto, últimamente muchos gobiernos y compañías se han esforzado en promover el desarrollo y la utilización de los estándares abiertos. Incluso Microsoft, que siempre ha sido referente de estándar cerrado, ha abierto especificaciones intentando convertirse en estándar.

Ejemplos de estándares abiertos:

Software: HTML / XHTML, PDF/X, PDF/A, OpenDocument, GIMP.

Hardware: ISA, PCI, AGP

Sistemas operativos: LINUX

Formatos: PDF, TXT, JPEG, PNG, Theora, FLAC.

Interesante información al respecto en:

<http://www.openformats.org/es> (información sobre formatos abiertos)

<http://www.fsf.org/> (Fundación para el software libre)

<http://www.gnu.org/philosophy/categories.es.html> (definiciones acerca de tipos de software: libres, semilibres, privativos, comerciales, etc.)

3.11 Normalización

También llamada “extracción de datos” es la puesta en práctica de la “confianza en estándares” descrita anteriormente.

Como un depósito digital cuenta con muchos tipos de archivos digitales, se debe elegir un formato para cada grupo de archivos del mismo tipo, normalmente se optará por el que entregue mejores posibilidades de longevidad, funcionalidad y preservación; se evitarán de esta manera problemas de complejidad y coste.

La normalización puede suceder en dos niveles:

- Formatos de archivos: Por ejemplo, el archivo decide almacenar todos sus documentos de imágenes en TIFF, entonces convertirá a este formato las imágenes que estén en otros, como PNG o JPG. Reducir el número de formatos reduce también la complejidad de la supervisión y las tareas al momento de realizar la migración. No obstante, los cambios de formatos algunas veces llevan consigo la pérdida de algunos elementos de los objetos digitales.
- Formatos de documentos: sucede muchas veces que un mismo documento contiene más de un formato (por ejemplo el archivo de un periódico digital almacena documentos que pueden contener a la vez texto, imagen, animaciones, etc.) entonces la manera para normalizarlo puede ser convertirlo todo a lenguaje SGML o XML, delimitado por un



DTD (Document Type Definition) común y que se ajuste a sus necesidades. Incluso un archivo podría convertir todos sus documentos a un DTD común reduciendo considerablemente los problemas de documentación y migración.

La Normalización pretende que la representación del contenido pueda ser ajena a aplicaciones informáticas específicas y que sea posible lograrla con algún software abierto que pueda ir cambiando fácilmente con los avances de la tecnología.

3.12 Emulación

La Emulación, al igual que la Migración, es considerada una de las técnicas más ricas y prometedoras para garantizar la longevidad de los objetos digitales.

Esta estrategia combina elementos de software y de hardware para reproducir en un contexto distinto al original las características esenciales del archivo. La idea principal es que un formato antiguo u obsoleto funcione en un ambiente informático nuevo que originalmente no reconoce al viejo formato.

Para llevar a cabo la emulación se requiere de un nuevo software, un emulador, el que traducirá los códigos e instrucciones desde el entorno computacional antiguo para que se ejecute correctamente en el nuevo. Para crear el emulador se utiliza la llamada "ingeniería inversa" del software original, que analiza todas las características de este con la finalidad de determinar de qué está hecho y de qué manera funciona. Profundizando en este estudio del funcionamiento se puede entender, modificar y mejorar las características del software.

Un emulador se diferencia de un simulador en que no sólo trata de reproducir el comportamiento del programa, sino que además intenta representar de manera precisa el dispositivo original.

La emulación se ha concretado en varios proyectos, entregando a menudo resultados prometedores. Sin embargo la técnica es un poco difícil de aplicar, puesto que alrededor de ella circulan una serie de cuestiones complejas, como las técnicas de la creación de los emuladores, los pasos administrativos para montar las especificaciones, la documentación de los sistemas que se emularán y las problemáticas legales que significan obtener los derechos de propiedad intelectual del hardware o software en cuestión.



Para muchos la emulación supone la mejor estrategia de preservar el contenido digital, aunque no sea posible conservar todas las cualidades de los objetos originales, al menos se puede mantener la mayor parte de su contenido y de su diseño.

La puesta en práctica de esta estrategia conllevaría:

- Cuando se desarrolle un software, habría que generalizar las especificaciones para que luego algún programa de emulación pueda interpretar los contenidos y hacerlos legibles en algún entorno informático futuro.
- Desarrollar las técnicas para guardar en metadatos legibles la información necesaria para encontrar, acceder y recrear los documentos digitales.
- Crear y desarrollar los procedimientos para encapsular el software, los metadatos y las especificaciones para la emulación. De esta forma se evitaría una posible disgregación de los datos en el futuro.

La idea de esta encapsulación es que siempre se guarden conjuntamente tanto el documento, como las especificaciones de su entorno informático. También se anima a los archivos a que en los metadatos incluyan todo el material explicativo posible, como procedencia, historia del ciclo vital, etiquetas, anotaciones, migraciones, como utilizar los archivos encapsulados, etc.

Por supuesto se debe garantizar que el bitstream de toda esta información será copiado textualmente cuando suceda una migración o cualquier tipo de renovación del sistema.

Si un software desarrolla toda esta documentación, el proceso de Ingeniería inversa resulta mucho más simple o incluso innecesario.

También, al igual que cualquier tipo de restauración actual, la emulación debe asegurar que el proceso pueda ser reversible sin ninguna clase de pérdida.

Para que un emulador sea efectivo, debe funcionar en cualquier plataforma computacional y aquí es donde nace uno de los principales problemas que tiene esta estrategia, y es que el software necesario para llevarla a cabo, el emulador, también es una aplicación que pertenece a un entorno informático determinado y por lo tanto sufre los mismos problemas que toda la información digital. Será entonces necesario preservar el emulador, el sistema operativo, la aplicación y los datos; si ocurriera la pérdida de alguno de estos componentes, puede suceder que la información también se pierda.



Un ejemplo de emulación es la que se practica en Linux para que funcione Microsoft Office, originalmente diseñado para Windows; en este caso se utilizan emuladores como Wine o CrossOver Office.

También podemos citar la emulación que tiene Macintosh Apple para reconocer archivos antiguos utilizados solamente en los computadores Apple.

Sin embargo hasta el momento los ejemplos de emulación más difundidos son los que se llevan a cabo para representar en computadores actuales los antiguos juegos que funcionaban en algún hardware ya casi obsoleto.

Ejemplos de algunas arquitecturas emuladas:

- Atari 2600
- Nintendo 64
- Game Boy
- PlayStation
- Sega Genesis

Ejemplos de emuladores de videoconsolas:

- MAME (Emulador de máquinas recreativas Arcade)
<http://www.mamedev.org/>
- Cyberstella (Emulador de la videoconsola Atari 2600)
<http://sourceforge.net/projects/stella/>
- zSNES (Emulador de la videoconsola Super Nintendo)
<http://www.zsnes.com/>

Más información sobre emulación:

<http://www.nla.gov.au/padi/topics/19.html>

<http://www.si.umich.edu/CAMILEON/>

http://es.wikipedia.org/wiki/Programa_de_emulaci%C3%B3n

3.13 Encapsulación

Como se explica en la estrategia de la emulación, la encapsulación es la técnica de agrupar un objeto digital con otros relacionados que son necesarios para proporcionar el acceso a ese objeto.

Esta estrategia apunta directamente a evitar la obsolescencia de la información digital, disminuyendo la posibilidad de que se pierdan los elementos necesarios para codificar y traducir los datos, puesto que los detalles acerca de cómo interpretar los bits en cualquier sistema futuro quedan registrados.



Para lograr la encapsulación pueden ser utilizadas estructuras físicas o lógicas llamadas “containers” o “wrappers” que proporcionan una relación entre todos los componentes de la información a preservar, tales como el objeto digital mismo, los metadatos, el identificador persistente y las especificaciones del software para la emulación. Este “envoltorio” puede describir los diversos objetos a través de un medio comprensible, como por ejemplo un documento XML. Un medio alternativo, y posiblemente más viable, es incluir una especificación del software o del hardware, o un enlace directo, de manera que más adelante se pueda reestablecer la información. Según el modelo de referencia OAIS, los objetos que deberían estar encapsulados son:

- La información para representar los bits apropiados para el acceso
- La procedencia, que describe la fuente del objeto
- El contexto, que describe cómo el objeto se relaciona con la información externa al contenedor
- La referencia, que proporcionará la manera para identificar inequívocamente el objeto
- La estabilidad, que dará la seguridad de que el objeto no ha sido alterado.

Es posible que ocurra el caso de que existan muchos objetos similares, con el mismo formato, legibles con el mismo software y que podrían ser codificados de la misma manera; para esta situación existe la alternativa de incluir un indicador que lleve a un solo depósito centralizado para toda esa información, de esta manera se ahorraría una gran cantidad de trabajo.

Para la emulación, se ha creado un formato específico, UPF (Formato de Preservación Universal) y su objetivo es que los objetos sean independientes de las aplicaciones y de los sistemas operativos envolviendo sus contenidos en metadatos “autodescriptivos” que incluyan las especificaciones técnicas para tener acceso a los materiales encapsulados.

El modelo de referencia OAIS plantea también un sistema de encapsulación, proponiendo que la incorporación de archivos y sus respectivos metadatos estén almacenados en paquetes de información, los AIP descritos anteriormente. Los metadatos pueden estar incluidos directamente con el objeto en el archivo o asociados a éste dentro del sistema. Otros modelos o programas de preservación digital que tienen la encapsulación como su principal estrategia son:

VERS (Victorian Electronic Records Strategy)

<http://www.prov.vic.gov.au/vers/vers/default.htm>



DIGITAL ROSETTA STONE

<http://www.ercim.org/publication/ws-proceedings/DELOS6/rosetta.pdf>

Para muchos documentalistas e informáticos que llevan investigando desde hace años el problema de la preservación digital, la encapsulación en conjunto con la migración, son las mejores, o incluso las únicas, estrategias a largo plazo que realmente pueden hacer frente al problema de la pérdida irremisible de la información. No obstante para otros, esto es todavía una ilusión, puesto que no se ha probado totalmente su implementación y porque, aún estando encapsulada la información, no soluciona de manera definitiva el problema básico del cambio de tecnología, puesto que habría que encontrar un nuevo medio de acceso.

Más información en:

<http://www.nla.gov.au/padi/topics/20.html>

http://www.digitaleduurzaamheid.nl/bibliotheek/docs/white-paper_xml-en.pdf (XML en la preservación)

3.14 Computador virtual universal (UVC)

Esta estrategia aún es más teoría que práctica, pero de llegarse a aplicar globalmente, los resultados serían satisfactorios para muchos tipos de información en peligro de desaparecer.

Técnicamente, el computador virtual universal es una representación virtual de una computadora simplificada que permite guardar información actual codificada y descifrarla en el futuro.

Para funcionar, esta estrategia utiliza elementos de la migración y de la encapsulación aunque para muchos es considerada una manera de emulación, que es llevada a cabo por un programa independiente de cualquier aplicación de software o hardware actual. Este programa registra desde un principio la arquitectura básica de cada computador para luego simular sus memorias, secuencias de registros y la manera de conectarse entre ellos, para de este modo, y a través de su decodificador de formatos, reconstruir el archivo en su aspecto original.

El UVC en el futuro debería poder leer todos los archivos de manera sencilla, para lo que se necesitaría una simple aplicación de emulación entre el UVC y el computador de la época.

Específicamente, el proceso de preservación de esta estrategia se desarrolla de la siguiente manera:



En el momento en que los objetos digitales son archivados se les aplica un esquema lógico que represente un tipo de datos junto a un programa decodificador capaz de interpretar el objeto de acuerdo con ese esquema.

Luego para restaurar el objeto se debe implementar un emulador de la UVC en una plataforma disponible, este ejecutaría el programa decodificador archivado que va a interpretar el objeto conservado entregando los datos a un programa de restauración que nos dará la representación del objeto según el esquema lógico archivado.

Esta estrategia presenta muchas ventajas, entre ellas:

- Preserva tanto archivos como software
- Ahorra trabajo al ser una sola la plataforma intermedia para muchos programas informáticos.
- Sus especificaciones son sencillas, por lo que no serían totalmente necesarios profesionales informáticos de alto nivel.
- Todo el proceso puede ser ensayado en el presente para comprobar comportamientos futuros.

Pero también tiene desventajas:

- Cuando archivamos es necesario elaborar métodos de codificación o programas de interpretación nativos de UVC para cada tipo de datos.
- Hay que desarrollar pronto decodificadores de archivos que posiblemente quedarán obsoletos en el corto plazo.
- Posiblemente sea necesario obtener información de los productores, y quizás, al no haber suficiente motivación comercial, esto sea difícil de conseguir.
- Es probable que algunos datos originales sean alterados en los procesos de codificación, esto puede hacer que se pierdan características esenciales del original.

Como para la mayoría de las instituciones la implementación del UVC está aún fuera de sus posibilidades, se recomienda mientras guardar cada archivo asociado con la mayor cantidad posible de metadatos.

Más información en:

http://www.kb.nl/hrd/dd/dd_onderzoek/reports/4-uvc.pdf (documento original de quienes desarrollaron esta idea, de 2002)

<http://www.digitaleduurzaamheid.nl/bibliotheek/docs/TDUVCv1.pdf> (explicación técnica del UVC)



http://www.kb.nl/hrd/dd/dd_onderzoek/uvc_voor_images-en.html (explica la funcionalidad del UVC para los formatos de imágenes)

3.15 Canonicalización

Dentro de los planes de preservación digital, algunos procesos son claves, como el seguimiento de la autenticidad o la mantención de la integridad de los objetos digitales, como se verá en las siguientes estrategias.

La Canonicalización tiene relación con esto, puesto que es una técnica para saber si en la transferencia de un formato a otro, el documento ha conservado todas sus características. Para conseguir esto se intenta crear un modelo con características comunes para cada tipo específico de ficheros. Luego, mediante estas claves, y a través de algoritmos canónicos, se puede comprobar si un fichero ha conservado su esencia una vez que se haya practicado la migración a nuevos formatos. Específicamente la canonicalización proporciona un lenguaje para entender los efectos de la traducción de los formatos.

Es por esto que la Canonicalización postula a ser considerada como una prueba fundamental para medir integridad en la estrategia de la migración, no obstante, aún no se ha llevado a cabo totalmente.

Más información en:

<http://www.dlib.org/dlib/september99/09lynch.html>

3.16 Control de la autenticidad

Esta estrategia está pensada como control de calidad de los documentos que serán preservados para asegurar la legitimidad de la información digital. Lo digno de confianza que pueda resultar un archivo y su contenido a lo largo del tiempo son cualidades que dan valor a un documento y que a la vez lo transforman en pieza fundamental para la formación de las generaciones futuras. El control de la autenticidad de los documentos digitales cobra vital importancia para todo tipo de archivo y en especial para aquellos que se utilizarán con fines legales, financieros o científicos.

Actualmente es fácil intervenir archivos digitales de texto, videos o fotografías, dejando la posibilidad de que existan varias versiones del mismo documento. En Internet se encuentran demasiados casos de documentos falsos o que han sido intervenidos sin la autorización de los creadores, ya sea para manipular información relevante o simplemente por diversión.



Antiguamente las fotografías eran consideradas pruebas policiales relevantes y muchas veces determinantes para la solución de algunos casos, en cambio hoy en día una fotografía no garantiza necesariamente la aclaración de un asunto policial debido a lo fácil que es intervenirlas digitalmente.

También algunos métodos para convertir, migrar, transmitir o restaurar los objetos digitales pueden tener como consecuencia la distorsión de la información por lo que también ocurriría la pérdida de la autenticidad.

Es necesario que un archivo compruebe con la mayor rigurosidad posible la procedencia de los documentos que a él ingresan, o que dentro de él se transforman, para así evitar tanto la publicación de información errónea como posibles problemas legales. Todo esto determinará el grado de confiabilidad que tenga un archivo documental.

Algunas medidas de control de autenticidad que un archivo debe tener son:

- Documentar la procedencia y la historia del documento digital.
- Utilización de metadatos de preservación que documenten la identidad y la integridad del objeto.
- Evaluación periódica y pruebas de autenticidad de sus documentos.
- Documentación de cada uno de los cambios que sufre un objeto digital.
- Utilización de marcas de agua o filigranas digitales que dificultarán el copiado desautorizado.

Finalmente, es necesario agregar que la autenticidad de un documento puede perderse debido a “buenas intenciones” de parte de los archiveros o investigadores, quienes podrían intentar mejorar la calidad de algunos documentos para una mejor visualización, pero alterando la estética original. Por ejemplo, si se intenta retocar los grises de una película antigua, con técnicas modernas, esta podría verse mejor y mostrar incluso más detalles, pero quizás se perderían algunos efectos deseados por los creadores o bien, alguna característica que identifique a las películas de ciertas épocas, como el alto contraste o los movimientos más rápidos. Por tanto, si se quiere realizar un cambio tal, es necesario que el original se siga manteniendo.

3.17 Control de la estabilidad o integridad

Esta estrategia se relaciona directamente con el control de la autenticidad puesto que mantener la integridad supone mantener el contenido auténtico de las ideas de los creadores de los documentos.



El mantenimiento de la integridad garantiza que cualquier documento no experimente una alteración que cambie su significado.

Los riesgos que sufren la integridad y la autenticidad son los mismos, es decir, la facilidad con que un documento digital puede ser modificado. Existen muchas maneras de que esto suceda:

- Errores humanos
- Errores naturales que se producen en los sistemas de almacenamiento
- Deterioro de los soportes
- Virus informáticos
- Modificaciones malintencionadas de hackers, piratas informáticos o cualquier persona que tenga acceso a los archivos

Es cierto que se necesita mantener la integridad del material original, pero esto está en constante enfrentamiento con la necesidad de la restauración, migración y actualización de los datos, lo que conlleva muchas veces la inevitable alteración de estos. Por tanto, la tarea es encontrar el criterio adecuado para mantener en la mayor medida posible la integridad original.

Para intentar mantener y comprobar la integridad de los documentos digitales, existen diversas estrategias que se pueden complementar entre sí:

- Firmas digitales: permiten que el documento haya sido comprobado por el autor, dando su consentimiento de que este mantiene sus características originales. La firma también la puede crear el archivo o depósito, de esta manera es la institución que preserva la que verifica y publica la integridad y autenticidad del contenido digital.
- Utilizar metadatos de preservación que incluyen las verificaciones de integridad de los documentos.
- Documentar cada una de las transformaciones que sufren los documentos y conservar las anteriores versiones, permitiendo la reversibilidad de estos cambios.
- Sumas de verificación (checksum): es una medida muy simple para comprobar la integridad de los datos. Este proceso consiste en sumar cada uno de los componentes básicos de un documento, generalmente los bytes, guardando el resultado. Luego, cuando se quiera realizar la comprobación, se lleva a cabo el mismo proceso y se comparan los resultados. Ambas sumas deben coincidir, lo que la mayor parte de las veces indica que el contenido del documento no ha sido alterado.



Este proceso se puede combinar con el algoritmo de reducción criptográfica MD5 (Message-Digest Algorithm 5) que permite verificar si los contenidos descargados desde Internet son fieles a sus originales.

Estas medidas serán cada vez más necesarias pues la transferencia de documentos digitales entre archivos seguramente será más frecuente, por lo que también aumentará la necesidad de comprobar la integridad y autenticidad de los datos.

<http://www.ietf.org/rfc/rfc1321.txt> (detalles técnicos del MD5)

<http://es.wikipedia.org/wiki/MD5> (explicación simple en español)

http://www.library.yale.edu/iac/DPC/AN_DPC_FixityChecksFinal11.pdf
(documento de la Universidad de Yale acerca de la integridad y los algoritmos de encriptación)

Algunos archivos se enfrentan muchas veces a la problemática de preservar paquetes grandes de información, ante lo cual, en algunas ocasiones, se opta por guardar tan solo una muestra. Si no hay problemas de espacio en el depósito, es preferible conservar los elementos completos para de esta manera mantener la integridad de la información en relación al contexto.

Por su parte, la integridad de los metadatos debe ser atendida de la misma manera que la del objeto mismo.

A estas medidas se tienen que sumar las medidas propias de la protección de los datos, tales como las asignaciones claras de responsabilidades en el personal, el mantenimiento de los equipos y todas las estructuras técnicas, el almacenamiento en condiciones adecuadas, las periódicas transferencias, las copias de seguridad almacenadas en lugares distintos, etc.

3.18 Metadatos de preservación

Con la irrupción del mundo digital, las reglas de descripción bibliográfica y catalogación de documentos que habían sido utilizadas por las bibliotecas y archivos desde hace más de un siglo, tuvieron que ser reanalizadas, puesto que estas normas ya no podían ajustarse a los nuevos documentos. Esto por una simple razón: en los archivos digitales no es tan fácil asociar el contenido del documento con su soporte.



Por tanto, se decide aplicar los metadatos, elementos que acompañan al documento digital, clasificándolo y describiéndolo para así facilitar su identificación y recuperación.

En reiteradas ocasiones se les ha definido como: “datos acerca de los datos” haciendo alusión al entorno numérico.

Además de las funciones de clasificación y descripción, los metadatos aportan información específica para intentar recrear el entorno informático original, haciendo frente a la facilidad de alteración que todo documento electrónico tiene.

Una de las iniciativas más importantes para estandarizar los metadatos sin duda es Dublin Core. <http://dublincore.org/> que ha tenido bastante éxito y se ha internacionalizado por su simpleza, interoperabilidad y por ser adaptable a cada tipo de necesidad bibliotecaria. Dublin Core propone 15 metadatos fundamentales que deberían acompañar a cualquier elemento, estos datos se agrupan en tres esferas: contenido intelectual, propiedad intelectual e instanciación.

En contenido: título, claves o tema, descripción, fuente, lenguaje, relación y cobertura.

En propiedad intelectual: autor o creador, editor, otros colaboradores y derechos.

En instanciación: fecha, tipo de recurso, formato e identificador.

Pero un documento digital además debe ser periódicamente revisado, lo que ha hecho necesario que se incluyan otro tipo de información además de la descriptiva. Para estos fines, la iniciativa que más se ha generalizado es la norma METS (Metadata Encoding and Transmission Standards), que propone tres tipos de metadatos:

- Descriptivos
- Administrativos
- Funcionales

Si bien, estos metadatos ofrecen mejoras sustanciales que favorecen la preservación, no son metadatos destinados específicamente a ella, por lo que algunos han intentado agregar una cuarta categoría destinada a la preservación.

Por su parte, la UNESCO ha propuesto otra clasificación de metadatos, los que sí incluyen la preservación. Estos son:



Metadatos de descubrimiento de recursos

- Metadatos de gestión de recursos
- Metadatos de preservación.

Desde hace algún tiempo, se intenta establecer los metadatos de preservación como un sistema aparte, que contenga información de todos los demás:

Datos descriptivos, para localizar; técnicos, para visualizar y utilizar; administrativos, para el control de la integridad y autenticidad; legales, para evaluar las posibilidades y limitaciones de uso.

Los metadatos de preservación también deberán referirse al entorno técnico del documento: procedencia, estrategias de preservación ya aplicadas, aspectos legales, etc. De esta manera se impulsará a que se mantenga en el tiempo la legibilidad, accesibilidad y autenticidad del documento.

Keefery Gallart señalan “Los metadatos de preservación permiten que un recurso digital se auto-documente durante cualquier fase de su ciclo vital, sea cual sea el entorno legal, técnico o institucional”

Desde al año 2005, la propuesta de metadatos de preservación más desarrollada y con más aceptación es PREMIS (PREservation Metadata Implementation Strategies). Esta iniciativa, patrocinada por OCLC y RLG, desarrolló el Data Dictionary for Preservation Metadata en 2005, dejándolo un par de años para que diferentes instituciones hicieran sugerencias. A raíz de esto, en marzo de 2008 ha aparecido la nueva versión 2.0.

<http://www.loc.gov/standards/premis/>

El diccionario establece un grupo fundamental de metadatos de preservación, además de un análisis de sus opciones de codificación, almacenamiento, gestión e intercambio. El objetivo final es conseguir un consenso internacional acerca del uso de los metadatos de preservación.

Debido a la lentitud y los costes que significan la adición, revisión y mantenimiento manual de metadatos, desde hace algún tiempo se está intentando que este proceso sea automatizado.

Por esta misma razón, algunas instituciones sólo reciben material si este ya posee los metadatos incluidos, comprobando que estos estén en correcto estado.



Una interesante iniciativa es el proyecto JHOVE, creado colaborativamente entre el sistema JSTOR y la Biblioteca de la Universidad de Harvard, desarrolla un sistema que automatiza la identificación, validación y caracterización de los formatos en el momento en que estos ingresan a un repositorio.

Página oficial del Proyecto JHOVE
<http://hul.harvard.edu/jhove/index.html>

Los metadatos pueden estar encapsulados con el mismo documento, en un documento independiente, o en ambas partes. En espera de que se normalice la manera de incluir los metadatos, lo ideal es hacerlo con la última opción, pero esta manera de aplicar ambos procedimientos es necesario mantenerla bajo un exhaustivo control, puesto que cualquier error puede generar versiones diferentes en cada lugar.

Tener los metadatos en un sitio distinto tiene por una parte el riesgo de que se pierda la vinculación con el objeto, y por otra, el inconveniente de que los datos, al estar en un fichero también digital, una base de datos, deberán someterse al mismo proceso de preservación. Sin embargo, esta medida permite la localización rápida del recurso a través de motores de búsqueda, sin entrar directamente en el documento mismo.

Las bibliotecas nacionales más comprometidas con la preservación han decidido, por el momento, mantener los metadatos en ficheros aparte, incluso en algunos casos, mantenidos fuera del depósito mismo.

Más información acerca de los metadatos y su papel en la preservación digital en:
<http://eprints.rclis.org/archive/00007682/01/final.pdf>

4. Medios de almacenamiento y sus cuidados

Debido a la gran cantidad de datos que un programa de preservación debe custodiar y gestionar, se hace necesario buscar más de un medio de almacenamiento.

En condiciones ideales, un archivo debería tener una capacidad suficiente en discos duros para poder guardar toda la colección, de manera que se pueda acceder automáticamente y en línea a toda ella; y además, tener otros dispositivos de almacenamiento en donde estén los documentos respaldados.

Pero normalmente la cantidad de ficheros y el gran espacio virtual que estos utilizan para ser almacenados en óptimas condiciones obligan a que muchos documentos estén guardados solamente en otros tipos de dispositivos, depositados en almacenes físicos y a los que hay que acudir manualmente.

Los soportes de almacenamiento de datos digitales se pueden separar en dos grandes grupos: magnéticos y ópticos, los que se diferencian por el modo de grabación, almacenamiento y recuperación de los datos.

4.1 Soportes Magnéticos

Son aquellos que a través de las atracciones y repelencias de los materiales férricos que los componen, permiten registrar, almacenar y reproducir información análoga y digital.

En un principio eran utilizados solamente para grabaciones sonoras, luego se amplió al video y actualmente se pueden almacenar en ellos cualquier tipo de dato digital.

Para muchos, los soportes magnéticos son la mejor alternativa para la conservación de la información, puesto que, por una parte tiene la precisión del mundo digital que entre otras alternativas permite realizar copias sin pérdidas, o cuantificar exactamente cualquier error, y por otra, tienen una degradación paulatina, por lo que se pueden tomar medidas con anticipación de acuerdo a cada tipo de daño.

Sin embargo, en el caso de las cintas, su lectura y búsqueda de datos es más lenta al ser secuencial, a diferencia de los discos, que utilizan una lectura aleatoria.



Un soporte magnético puede ser un disco o una cinta, a continuación se describen brevemente los más utilizados en los últimos años:

- **Discos**

Discos duros: dispositivo que se compone por una o varias láminas rígidas de forma circular recubiertas con un material que posibilita la grabación magnética de datos. Los podemos encontrar en computadores (de sobremesa o portátiles), o en su versión Microdrive (cámaras digitales, agendas electrónicas y otras tecnologías similares), que normalmente es de menor capacidad.

Disquete de 3 ½: disco de almacenamiento extraíble que se compone de pequeños discos de material plástico flexible. Actualmente están casi totalmente en desuso por su baja capacidad y velocidad de lectura, sin embargo, vale su mención al ser muy utilizados durante años, lo que ha generado que algunas instituciones aún guarden información en este formato.

Discos Zip: disco extraíble, de apariencia parecida al disquete de 3 ½, pero con capacidad de almacenamiento y velocidad de escritura y lectura mucho mayor.

Otros discos no tuvieron mucho éxito en el mercado, intentaron superar al disquete de 3 ½ agregando más capacidad, pero llegaron en un momento en que el aumento de la memoria crecía muy rápido, por lo tanto, al no superar los 2 GB, quedaron rápidamente obsoletos, ejemplos de estos son los dispositivos JAZ, SYQUEST y SUPERDISK.

Hay que señalar también los discos RAID, o Arrays de discos duros, que son la combinación de varios discos que permiten una alta capacidad de almacenamiento y disponibilidad en línea. Para el usuario, la información pareciera que está contenida en un solo lugar.

http://www.technick.net/public/code/cp_dpage.php?aiocp_dp=guide RAID
(explicación profunda acerca de RAID)

<http://es.wikipedia.org/wiki/RAID> (artículo de Wikipedia)

- **Cintas**

Existen muchos tipos de cintas magnéticas, en este estudio nos centraremos tan solo en aquellas que permiten almacenamiento digital y que actualmente son utilizadas por muchas empresas e instituciones para respaldar amplias cantidades de contenidos.



DAT (Digital Audio Tape): la mayoría fabricadas en Poliéster. Son utilizadas normalmente para el almacenamiento digital de audio. Permite el copiado sin pérdida, pero sus altos costes han hecho que sea reemplazada por los CDs o DVDs, que tienen similares tasas de muestreo.

Después de muchos intentos de estandarización, se establecieron dos tipos, que son los más comunes:

S-DAT: de cabeza estacionaria (lectura lineal) 90 minutos de duración.

R-DAT: de cabeza rotatoria (lectura helicoidal) 120 minutos de grabación.

DAT/DDS (Digital Data Storage): utilizando los mismos cartuchos DAT, esta cinta desarrollada por Sony y Hewlett Packard, almacena cualquier contenido digital. en 2007 se presentó el DAT 160 que permite almacenar hasta 80 GB y 160 GB con una compresión sin pérdida de 2:1. Muy próximo a cobrar importancia en el mercado está el DAT 320.

Más información en: <http://www.datmgm.com/>

DLT (digital linear tape): también tiene su versión Súper DLT (SDLT). Desarrollada originalmente por DEC en 1984 y actualmente adquirida por Quantun Corporation. Alcanzó una capacidad máxima de 800 GB, ampliable a 1,6 TB en sus versiones DLT-S4 y DLT-S4A. Desde 2007 se dejó de fabricar por bajas ventas en el mercado, entregando su tecnología al formato LTO.

Más información en: <http://www.dlftape.com/>

LTO (Linear Tape Open): proviene del formato original ULTRIUM, estrenada el año 2000 y que almacenaba hasta 100 GB. Fue desarrollada por IBM, Seagate y Hewlett-Packard para ser formato abierto de almacenamiento. A la fecha de este estudio, su última versión es el LTO-4, desarrollado en 2007 y permite guardar 800 GB de información sin comprimir. Actualmente esta tecnología es fabricada por muchas empresas, además de las creadoras, como Sony o TDK.

Más información en: <http://www.lto-technology.com/default.php>

VXA: creada por Ecix y actualmente manejada por Tandberg Data. Esta tecnología ofrece una lectura denominada "packet", que contrasta con la tecnología lineal de sus competidores. A la fecha, su última versión es el VXA-3 (2005) y alcanza una capacidad de 160 GB.

Más información en:

<http://www.vxa.com/index.html?CFID=1792728&CFTOKEN=26185480>



AIT (Advanced Intelligent Tape): esta cinta de alta capacidad es totalmente desarrollada y controlada por Sony y compite con los formatos descritos anteriormente. Su aspecto es igual al Video8. Tiene una versión Súper AIT (SAIT) que en su versión SAIT-2 (2006) entrega una capacidad máxima de 800 GB.

Más información en: <http://www.aittape.com/>

QIC (Quarter-Inch Cartridge): desarrollado por 3M, ha sido ampliamente utilizada aunque últimamente ha sido reemplazada por otras cintas con más capacidad, la QIC tan solo alcanza los 25 GB. Se diferencia de las demás por tener un sistema de arrastre que protege más la integridad de la cinta.

Más información: <http://www.qic.org/>

Otro producto que se comercializa son las bibliotecas multicinta, o librerías de cintas de alta capacidad, que en su totalidad pueden superar los 50 TB de almacenamiento sin compresión. Estas bibliotecas ocupan algunas cintas de las descritas anteriormente. Sus costes, en relación a la alta capacidad, no son muy elevados.

Los ejemplos más utilizados son:

- IBM TotalStorage <http://www-03.ibm.com/systems/es/storage/>
- HP StorageWorks
http://h18000.www1.hp.com/storage/disk_storage/msa_diskarrays/san_arrays/index.html

4.1.1 Problemas que afectan a los soportes magnéticos

Hay una serie de factores que pueden deteriorar este tipo de soportes.

Quizás el problema más habitual es el llamado “flaking off”, una especie de descascarado que se genera por la expansión y contracción de las capas del soporte. Esto es producido cuando las condiciones de humedad y temperatura no son las óptimas o cuando hay cambios bruscos en ellas.

Por otra parte, la humedad excesiva puede producir hongos, los que deterioran rápidamente el aglutinante que mantiene unidas las partículas magnéticas. Estos hongos también pueden liberar esporas, que afectarían a los documentos magnéticos cercanos.

Otros factores también pueden deteriorar estos materiales, como la acumulación de polvo, los campos magnéticos cercanos o la tensión excesiva de las cintas.



4.1.2 Sugerencias para la conservación de los soportes magnéticos

- Limpiar frecuentemente los equipos, esto ayuda a eliminar el polvo, las sustancias que desprenden los propios equipos y las esporas que propagan los hongos.
- Almacenar en condiciones óptimas de temperatura y humedad. Las investigaciones acerca de los valores adecuados difieren mucho en diversas fuentes, como IFLA, UNESCO o algunas cadenas de televisión, al comparar encontramos un amplio rango de diferencia, que varía entre 5 y 20° C en temperatura, y entre 20 y 45% de humedad relativa. Lo más importante es que las condiciones elegidas sean estables.
- Mantener alejado cualquier campo magnético
- Utilizar deshumidificadores
- Evitar los elementos propensos al fuego, como estanterías de madera o materiales combustibles
- No utilizar excesiva luz y asegurarse que la radiación ultravioleta esté bajo los 75 microwatios. De preferencia mantener siempre el almacén en oscuridad mientras no se esté utilizando.
- Tener uno o varios sistemas antiincendios; si es posible, evitar los aspersores, que pueden causar grandes daños a los documentos.
- Almacenar las cintas verticalmente.
- Distensionar las cintas si pasan mucho tiempo inutilizadas.
- Si es posible, fijar las lengüetas de protección contra escritura.

4.2 Soportes ópticos

Cuando nos referimos a estos soportes, estamos hablando de los discos ópticos creados a principios de la década de los 80 por las empresas Sony y Phillips y diseñados exclusivamente para el registro y la lectura de información digital.

Los discos tienen un tamaño estándar de 12 centímetros (existen algunos de 8 centímetros, ya casi extinguidos) y se conforman de varias microláminas metálicas superpuestas protegidas por una estructura de policarbonato. Las microláminas en su mayoría son de aluminio, aunque las hay de platino y oro, que presentan mejores posibilidades de conservación pero también mayor coste.

Los datos se registran en microsurdos, llamados *pits*, que siguen una espiral continua que va desde el centro hacia fuera, estos surcos direccionan el haz láser que interpreta el contenido. El registro puede ser por uno o por ambos lados del disco.

La ventaja que presentan estos soportes es variada:



- Permiten el registro de una gran cantidad de datos (millones de páginas de texto)
- Al ser pequeños, su almacenamiento es fácil.
- En condiciones óptimas de almacenamiento, pueden durar muchos años
- No hay roces mecánicos en su escritura/lectura.
- En el caso de grabaciones de audio, estas no presentan ruido residual

Los soportes ópticos se pueden clasificar en tres grandes grupos:

- Discos ROM (Read Only Memory) Son estampados desde la fábrica. Los formatos más extendidos son el CD-ROM de música y el DVD-ROM de películas.
- Discos de grabación única WORM (Write Once Read Many), Se comercializan para que el usuario pueda grabar lo que necesite. Esta grabación no puede ser borrada ni reescrita, aunque sí se puede grabar en varias sesiones.
- Discos reescribibles o de grabación múltiple. Como su nombre lo indica, en él se pueden borrar los datos y grabar muchas veces. Estos discos no han presentado buena calidad y su aceptación en el mercado no ha sido buena, por lo que para conservación de datos, se recomiendan los discos WORM.

Los discos más utilizados hasta el momento, sin duda son el CD y el DVD, con varias versiones cada uno, diferenciados por su capacidad de almacenamiento, grosor y detalles de estructura.

El DVD, al usar *pits* más pequeños, presenta mayores posibilidades de almacenamiento (más de 17 GB) y mejor capacidad para corregir errores que los CDs, sin embargo su valor comercial aún es más elevado.

Desde hace años existe la búsqueda entre las grandes empresas fabricantes para poner en el mercado el sucesor del DVD. Esto derivó en dos grandes formatos, el HD-DVD, desarrollado principalmente por Toshiba y el BLUE-RAY, cuyo principal gestor es Sony. Este último formato ganó la batalla al ser retirado su oponente del mercado. Por lo que para muchos, el BLUE-RAY es el nuevo gran formato óptico. Su capacidad actualmente llega a 50 GB y los fabricantes prometen ampliarlo en el corto plazo. Sin embargo su entrada en el mercado aún no ha sido masiva, al ser altos los precios tanto de los discos como de los lectores.

Para más información acerca de estos formatos y sus derivaciones, las definiciones en Wikipedia son muy completas y enlazan con otras páginas relevantes.



CD <http://es.wikipedia.org/wiki/Cd>

DVD <http://es.wikipedia.org/wiki/DVD>

BLUE-RAY http://es.wikipedia.org/wiki/Blue_Ray

4.2.1 Problemas que afectan a los soportes ópticos

Pese a que la historia de estos formatos es aún muy corta, por ejemplo en relación a las cintas magnéticas, ya se pueden identificar las principales causas de su deterioro.

Enumeramos acá las más frecuentes:

- Temperaturas extremas (sobre todo calor) y humedad relativa extremas.
- Exceso de iluminación.
- Materias grasas en el reverso, como las que pueden dejar las huellas digitales.
- Exceso de polvo.
- Impurezas contenidas en el aire (sulfuros, óxidos de nitrógeno).
- Arañazos, que producen surcos por donde pueden entrar el polvo u otras sustancias como las descritas anteriormente.
- Cualquier deformación física puede causar la variación del haz láser y por lo tanto la lectura errónea de la información.

4.2.2 Sugerencias para la conservación de los soportes ópticos

Al igual como sucede con los formatos magnéticos, las fuentes no coinciden en las condiciones de humedad y temperatura adecuada para conservar estos materiales. No obstante, la mayoría oscila entre 12 y 23° C y entre 25 y 45% de Humedad Relativa. Los estudios si coinciden en que cualquiera que sean las condiciones elegidas, estas deben ser estables. Dentro de las fuentes consultadas están UNESCO, IFLA y Kodak.

Algunas instituciones conservan sus materiales en temperaturas extremadamente bajas, pero esto solo es recomendable para la conservación a largo plazo que no incluya la consulta, y con unas condiciones muy controladas de humedad.

Además de estas condiciones ambientales, se sugieren las siguientes medidas:

- No manipularlos en exceso, y hacerlo tan solo de los bordes y el orificio central. Si es posible, utilizar guantes.
- Mantenerlos siempre en sus cajas originales cerradas, nunca dejarlos dentro de los equipos cuando no se estén utilizando.
- Evitar contactarlos con papeles, plásticos y espumas de goma, salvo que sean materiales inertes o libres de ácidos.



- No apilarlos, sino que almacenarlos verticalmente.
- Mantenerlos en dependencias oscuras cuando no sean utilizados.
- Las etiquetas deben ser de materiales no oxidantes y libres de ácidos. De ser posible, que no estén directamente en el disco sino en la caja.
- Evitar el uso de los discos reescribibles
- Nunca escribir en el disco.
- En su limpieza se puede utilizar agua con jabón, o con más recursos, nitrógeno o aire comprimido. Se recomienda un paño que no libere pelusas o bien toallitas diseñadas para estos fines. La limpieza no debe hacerse de manera circular, sino que axialmente o radialmente, por ejemplo, desde dentro hacia fuera. Las máquinas de limpieza por ultrasonido también son útiles para los discos ópticos.
- En caso arañazos, se pueden limpiar con cualquier limpiametales aplicándolo en pequeños círculos y siempre desde el interior hacia el exterior. Si estos son muy profundos, existen máquinas especiales que pulen la superficie de policarbonato.
- Según estudios, los discos que han presentado mayor resistencia y compatibilidad son los que utilizan como tinte la cianina (cyanine) estabilizada con metal (color azul verde). También son buenos los que utilizan phtalocyanine (azul pálido) y azo (azul profundo), aunque este último, creado por Varbatim, presenta algunos problemas de compatibilidad. El color puede engañar, por lo que es mejor ver las especificaciones del fabricante.
- Cuidar también la limpieza de los reproductores.

Los estudios predicen que si un disco óptico se almacena en óptimas condiciones, puede durar más de 100 años.

5. Cuestiones legales

Cualquier estudio acerca de preservación digital se encontrará, mas temprano que tarde, con las problemáticas legales que afectan directamente a las obras digitales almacenadas en los archivos y dispuestas a ser preservadas. Estos problemas se acrecientan debido a que cada país tiene su propia legislación, pero en cambio los documentos digitales, impulsados principalmente por Internet, potencialmente pueden ser vistos y utilizados en cualquier parte del mundo, lo que hace muy difícil que existan normas globales específicas para los diversos tipos de explotación que un documento digital pueda tener.

A todo esto se suma que la tecnología va creciendo a pasos de gigante, por lo que las leyes, los contratos, los derechos, las convenciones internacionales y todo elemento legal que involucre la gestión de los objetos electrónicos, también se debe ir adecuando a estos cambios, lo que habitualmente no sucede con la misma velocidad.

Hasta antes de la aparición de los recursos digitales, las leyes eran relativamente claras y específicas, cualquier persona podía adquirir comercialmente una obra, y era dueña de su soporte físico (libro, revista, escultura, cinta de video, etc.) pudiendo hacer con él lo que quisiera, sin embargo el contenido, la obra creativa, era propiedad intelectual privada de los creadores, por lo que se debía pedir autorización, normalmente pagando, para utilizar dicho contenido.

Con la creación, y sobre todo, la masificación de los recursos digitales, muchos sistemas legislativos se han visto obligados a cambiar una serie de leyes y agregar otras nuevas para dar cobertura a cada nuevo tipo de obra y a la explotación de ellas.

Todo este proceso de actualización y adecuación de las legislaciones comenzó a mediados de la década de los 90, desde entonces se han creado organismos específicos para el tema y muchos países han comenzado una cooperación para debatir y tomar medidas que sean justas para cada una de las partes involucradas, las que también han crecido de manera exponencial. Este proceso sigue en marcha y posiblemente durante mucho tiempo más, ya que la "industria de los contenidos" y las Tics al parecer están dando sus primeros pasos, pese a que pueda parecer que ya están totalmente establecidas.

Cuando se habla de las problemáticas legales que afectan a un programa de preservación digital, normalmente se piensa que lo que está en juego es



solamente el derecho de autor, y aunque es cierto que este conjunto de normas es el que más atañe al acceso a los materiales, hay también en escena otros actores legales, como el derecho de las instituciones a recolectar, preservar y proporcionar acceso a los objetos digitales, o el derecho que estas mismas instituciones tienen para establecer las condiciones de acceso y utilización. Por su parte en la mayoría de los países, la sociedad tiene el derecho de acceso a la información y a la cultura, así como el derecho a la libre expresión.

Todos estos aspectos legales involucrados se conjugan, complicando más aún el panorama que cada institución debe manejar rigurosamente, incluso antes de emprender la tarea de la digitalización y el almacenamiento digital que es la antesala a los programas de preservación.

Este documento intentará describir brevemente algunos asuntos legales involucrados directamente con los programas de preservación digital.

Es necesario volver a mencionar que cada país tiene sus propias leyes relacionadas con este tema, sin embargo por convenciones internacionales o simplemente por intuición, hay muchos aspectos que se relacionan.

De los tratados internacionales, el más destacado es el Convenio (o convención) de Berna (Suiza), que afecta a casi todos los países del mundo. Este funciona solamente si hay más de un país involucrado y explicándolo a grandes rasgos, protege la autoría las obras ajenas a un país como si fueran propias, reservando a cada país la facultad de aplicar sus leyes.

En este enlace se puede acceder al convenio:

<http://www.bibliotecasvirtuales.com/biblioteca/derechosdeautor/conveniodeberna.asp>

5.1 Derecho de autor

Son normas que habitualmente están bajo el cobijo de alguna Ley de Propiedad Intelectual y que otorgan protección a los creadores de obras, normalmente de índole científica o de cualquier rama de las artes.

Para que una obra sea protegida por este derecho, debe estar publicada o manifiesta de alguna manera tangible; las ideas no concretadas no se protegen.

Desde hace algún tiempo en muchos países ya ni siquiera es necesario registrar o inscribir la obra, basta con firmarla o expresar la autoría de algún modo.



Dentro de estos derechos existen los derechos morales y los económicos, los primeros abarcan facetas que se relacionan con la obra intelectual misma, como la protección de la integridad, el reconocimiento en la divulgación y el derecho de modificación de parte del autor. Los de explotación tratan las cuestiones que en alguna parte del proceso incluyen intereses económicos, como la distribución o la reproducción.

Existen también los derechos afines, que involucran a intérpretes, ejecutantes, entidades, etc.

Los derechos no imposibilitan el acceso a las obras, casi siempre se puede acceder a ellas consiguiendo licencias, un método para utilizar solamente los contenidos, sin comprar la obra. Las licencias se consiguen pagando o llegando a acuerdos. La utilización de las obras habitualmente tiene restricciones, tanto temporales como espaciales, es decir, se pueden utilizar solo en algunos lugares y durante un tiempo determinado.

Finalmente, existen las obras que están en el "Dominio público" ya sea por que los autores quisieron que así sea o bien porque ha pasado un tiempo legal determinado en la que los derechos privados pasan a ser públicos. Por ejemplo, en Europa, transcurridos 70 años después de la muerte de autor, la obra pasará a dominio público.

5.2 En qué afectan las cuestiones legales a la preservación

Un archivo digital no cumple toda su misión si tan solo custodia las obras sin ponerlas a disposición del público. Sin embargo, esto genera una serie de problemas legales, puesto que casi todas las fases del proceso de preservación, como el copiado, la reproducción, la transformación, el control de acceso, etc. intervienen en las protecciones legales de las obras.

Citamos acá algunos casos:

- Para obtener y respaldar el material, es necesario realizar copias. Lo que en si mismo ya viola los derechos de reproducción.
- El hecho de migrar lleva consigo, la mayoría de las veces, un acto de modificación que afecta a la integridad de la obra. Se viola así el derecho del autor a modificar o realizar obras derivadas.
- El acto de la digitalización altera muchas obras, lo que también modifica la integridad de ellas.
- Al poner a disposición en la Web los contenidos digitales, estos se están distribuyendo y exhibiendo.
- Un repositorio, por su esencia misma, controla el acceso a los contenidos, pudiendo introducir contraseñas o cifrados. De esta manera se altera el



derecho exclusivo que tienen los autores o distribuidores para controlar el acceso a su obra.

- En ocasiones, se limita el acceso, alterando los dispositivos utilizados por los productores.
- Modificar los ficheros puede en algunos casos atentar en contra de la integridad de una creación.

Todo lo anterior puede generar que las personas o instituciones titulares de los derechos, al ver alterados sus productos, se nieguen a autorizar su uso. Pero además hay otras situaciones legales que pueden entorpecer a los programas de preservación:

- Una serie de obras, tales como las audiovisuales, son realizadas colectivamente, por lo que los derechos también están repartidos, esto dificulta la negociación ya que puede ser difícil localizar a todos los titulares.
- Existen las llamadas “obras huérfanas”, de las cuales se desconocen sus autores, sin embargo estos pueden aparecer en cualquier momento, complicando la situación.
- Derechos de acceso y derechos de privacidad pueden contradecirse
- Como lo explicábamos anteriormente, muchas leyes no son claras al ser tan cambiante la escena de los contenidos digitales, por tanto, algunas situaciones legales pueden ser confusas.
- Tampoco son claras las medidas a tomar cuando se encuentran involucradas las jurisdicciones de varios países, por ejemplo cuando una obra se crea, inscribe, produce y exhibe en lugares distintos, es complejo saber a que marco jurídico acudir.
- Las negociaciones para adquirir derechos o licencias pueden llegar a ser muy costosas económicamente, lo que en muchos casos imposibilita la gestión de las obras.

Sin embargo, el panorama no es tan desalentador, puesto que también existen una serie de situaciones amparadas por la ley o por la buena voluntad, que permiten la recolección, utilización y preservación de los recursos:

- Algunas legislaciones autorizan el copiado y la utilización de las obras bajo ciertas condiciones, como por ejemplo, que no tengan ánimo de lucro o que sean destinadas a fines didácticos, educativos, patriotas, etc.
- Poco a poco las legislaciones se van sumando a la idea de autorizar la reproducción y el copiado con fines de conservación.
- Existe el depósito legal
- Son comunes las “herencias” que unas instituciones pueden recibir de otras similares.



- Muchos autores se benefician de la publicación de sus obras por los medios digitales, por lo que normalmente otorgan permisos a cambio del reconocimiento de la autoría.
- Acuerdos como el del caso anterior también se pueden establecer con empresas o instituciones que tienen a su cargo grandes cantidades de contenidos, estos pueden ser convenios de cooperación en las que el archivo se compromete a gestionar, preservar y controlar el acceso a los documentos a cambio de que se le cedan sus derechos.
- Cada vez se utiliza más la entrega voluntaria de datos a cambio de que estos se preserven.
- En Internet es común encontrar documentos publicados con permisos para el uso libre.

Además de todo esto, muchas personas e instituciones están intentando desde hace tiempo que se logre el acceso libre a toda la información que circula por Internet, para esto se han creado organismos especializados que están en constante lucha con las empresas, instituciones o personas que obtienen ganancias económicas de las obras.

Una conocida iniciativa creada en 1985 es la Fundación para el Software Libre, que incentiva a la eliminación de las restricciones que hay para copiar, distribuir o modificar las aplicaciones informáticas. Esta fundación también ha creado la licencia GNU GPL (General Public License) que se caracteriza por ceder algunos derechos a los usuarios e intentar resolver situaciones como ambigüedades, compatibilidades entre diferentes licencias, adaptaciones a diferentes marcos jurídicos, mal uso de las patentes de software, etc.

Su última versión es de junio de 2007. <http://www.gnu.org/licenses/gpl-3.0.html>

Otro proyecto a destacar es Creative Commons, una organización que a través de nuevas legislaciones y tecnologías pretende conseguir que todos o casi todos los derechos de explotación de las obras sean libres, por lo que no habría que pagar por hacer copias o publicaciones de los objetos digitales; ni siquiera sería necesario tener que contactar o localizar a los autores o encargados de los derechos. No obstante, estas licencias reconocen la autoría, obligando a citar a los creadores; impiden las modificaciones de las obras y exigen que las obras derivativas se distribuyan bajo la misma licencia del original.

Estas licencias han sido traducidas ya a varios idiomas y decenas de países ya las están incorporando.



Más información:

<http://creativecommons.org/> (sitio oficial)

<http://es.creativecommons.org/> (sitio español) <http://cyber.law.harvard.edu/blogs/gems/ion/secreativo.swf> (video animación explicativo de Creative Commons)

<http://www.arielvercelli.org/lcsdc.pdf> (libro *“La Conquista Silenciosa del Ciberespacio: Creative Commons y el diseño de entornos digitales como nuevo arte regulativo en Internet”*)

Por último, una iniciativa a destacar es Copyleft, también relacionada con GPU, es un grupo de derechos de autor que elimina restricciones tales como las de modificación o distribución que impone el copyright, pero manteniendo la referencia y los derechos del documento original.

Por lo tanto, Copyleft no es solo una licencia de la cual se benefician todo tipo de obras, como juegos, programas informáticos, artículos científicos, etc., sino que también es un incentivo para la creación colectiva, puesto que cualquiera puede ir aportando ideas y mejoras a las obras iniciadas por otros. Su simbología es opuesta a la del Copyright, la © pero abierta hacia la izquierda

<http://www.fundacioncopyleft.org/> (Fundación Copyleft)

<http://www.gnu.org/copyleft/copyleft.es.html> (explica más ampliamente Copyleft)

<http://www.manualcopyleft.net/> (manual de uso de Copyleft)

5.3 Sugerencias para abordar las cuestiones legales

La importancia de la labor que significa preservar el patrimonio digital es indiscutible, así como también la necesidad de agotar todos los medios posibles para lograr esta misión, sin embargo esta debe ser cuidadosa de no atentar contra los derechos legítimos que le corresponden a los autores y demás involucrados en la creación de las obras.

Cada programa de preservación debe conocer muy bien las legislaciones que están comprometidas con los documentos dispuestos a custodiar, para así elaborar estrategias aplicadas que le impidan verse involucrada en desagradables problemas legales a futuro.

A continuación algunos consejos sacados de la experiencia de archivos, bibliotecas y otras instituciones que gestionan material digital:

- Es recomendable contar con asesoramiento legal especializado en temas patrimoniales y de propiedad intelectual, que ayuden a conocer los



procedimientos, protocolos, limitaciones, estrategias y enfoques adecuados para cada situación específica de la gestión.

- De ser posible, identificar a todos los titulares o responsables de los derechos implicados en la colección, así como diferenciar las obras que están en el dominio público de las que están bajo titularidad de derechos.
- Comprobar que las partes implicadas en el proyecto también estén informadas de los derechos que están relacionados con las operaciones de preservación.
- Buscar estrategias de cooperación con instituciones y empresas involucradas para obtener beneficios mutuos.
- Verificar que todo el personal también comprenda las responsabilidades legales.
- Controlar mediante procedimientos seguros el acceso del personal a los archivos y a la realización de copias.
- Informar a los usuarios de los derechos que rodean a cada objeto digital y de sus obligaciones al respecto.
- En lo posible, establecer el contacto entre los usuarios y los titulares de los derechos.
- Utilizar programas informáticos de fuentes abiertas.
- Si es necesario, restringir el acceso a ciertos materiales más conflictivos desde el punto de vista legal, hasta que se solucionen los inconvenientes.
- Realizar una evaluación periódica de los procedimientos que involucren las cuestiones legales.
- Actualizarse de las modificaciones que pueden sufrir los derechos, como el cambio de titular o cuando caduque un plazo. Una buena estrategia es realizar un calendario o cronograma.
- Crear licencias estándar para cada clase de material, esto ayudará a ahorrar tiempo y el trabajo de negociar una a una las situaciones.
- Si es posible, separar los procedimientos de preservación de los demás usos y accesos a los materiales.
- Registrar en los metadatos los derechos comprometidos con el objeto o con el tipo de objeto.
- Promover la creación o la modificación de la legislación para facilitar la conservación de los documentos digitales.

Artículos que abordan cuestiones legales:

<http://www.rebellion.org/noticia.php?id=16983>

<http://www.arielvercelli.org/ccylpdc/>

<http://www.elmundo.es/navegante/2002/05/20/empresas/1021879870.html>

<http://www.liberalismo.org/articulo/321/69/monopolio/ideas/propiedad/intelectual/>

6. Buenas prácticas y sitios Web relacionados

Como se explicó en la introducción, muchas instituciones como bibliotecas, archivos, museos y universidades ya han están implementando programas de preservación digital o bien, entregan directrices o información relevante para llevarlos a cabo.

Acá se enumeran los que fueron consultados para este trabajo.

BRITISH LIBRARY <http://www.bl.uk/>

CAMILEON <http://www.si.umich.edu/CAMILEON>

CASPAR PROJECT <http://www.casparpreserves.eu/>

CLIR Council on Library and Information Resources <http://www.clir.org/>

CREATIVE COMMONS <http://creativecommons.org/>

CREATIVE COMMONS (España) <http://es.creativecommons.org>

CEDARS <http://www.leeds.ac.uk/cedars/>

CORNELL UNIVERSITY LIBRARY. *Digital Preservation Management: Implementing short-terms strategies for long-term problems.* (2004-2007)

http://www.icpsr.umich.edu/dpm/dpm-eng/eng_index.html

DLF Digital Library Federation <http://www.diglib.org/preserve.htm>

DIGITAL PRESERVATION COALICION. *The Handbook*

<http://www.dpconline.org/graphics/handbook/index.html>

D-LIB MAGAZINE <http://www.dlib.org/>

DUBLIN CORE <http://dublincore.org/>

FREE SOFTWARE FOUNDATION <http://www.fsf.org/>

FUNDACIÓN COPYLEFT <http://www.fundacioncopyleft.org/>

GNU <http://www.gnu.org/>

JHOVE PROJECT <http://hul.harvard.edu/jhove/index.html>

JISC, **Joint Information Systems Committee**. Apartado Preservación.

<http://www.jisc.ac.uk/whatwedo/programmes/preservation.aspx>

Library of Congress (LC) <http://www.loc.gov/index.html>

LOCKSS (Lots Of Copies Keep Staff Safe) <http://www.lockss.org/lockss/Home>

METS Metadata Encoding and Transmission Standards

<http://www.loc.gov/standards/mets/>

NARA National Archives and Records Administration <http://www.archives.gov/>

NATIONAL ARCHIVES, Apartado Preservación

<http://www.nationalarchives.gov.uk/preservation/advice/digital.htm>

NDIIPP National Digital Information Infrastructure and Preservation Program

<http://www.digitalpreservation.gov/>

OPENFORMATS <http://www.openformats.org/es>

PADI Preserving Access to Digital Information <http://www.nla.gov.au/padi/>



PANDORA Preserving and Accessing Networked Documentary Resources of Australia <http://pandora.nla.gov.au/>

PLANETS Preservation and Long-term Access through Networked Services
<http://www.planets-project.eu/>

PREMIS Preservation Metadata Implementation Strategies <http://www.oclc.org/research/projects/pmwg/>

RLG DIGINEWS

<http://www.oclc.org/programs/publications/newsletters/diginews.htm>

VERS <http://www.prov.vic.gov.au/vers/vers/default.htm>

Bibliografía de textos consultados

1. ADELSTEIN, Peter. *Media Storage, Quick Reference*. 2004
<http://www.climatenotebook.org/MSQR/MSQR.pdf>
2. ANGLADA I DE FERRER, Lluís Ma. *Biblioteca digital, ¿mejor, peor o distinto?* 2000
<http://eprints.rclis.org/archive/00014133/>
3. ARCHIVES NEW ZELAND. *Digitisation Standard Exposure Draft*. 2006
<http://www.archives.govt.nz/continuum/documents/Digitisation%20Standard%20Draft.pdf>
4. BARRUECO, José Manuel. *Preservación y conservación de documentos digitales*. 2004
<http://www.archivovirtual.org/seminario/ediciencia/pdf/CAPITULO7.pdf>
5. BEREIJO MARTINEZ, Antonio; FUENTES ROMERO, Juan José. *Los soportes fílmicos, magnéticos y ópticos desde la perspectiva de la conservación de materiales*. 2001
<http://www.um.es/ojs/index.php/analesdoc/article/viewFile/2411/2401>
6. CANDÁS ROMERO, Jorge. *El papel de los metadatos en la preservación digital*. 2004
<http://eprints.rclis.org/archive/00007682/01/final.pdf>
7. CASTILLO, José Manuel; JORBAN, Ferran. *Almacenamiento distribuido y preservación digital: Una panorámica de alternativas*. 2008
http://www2.ub.edu/bid/consulta_articulos.php?fichero=20casti2.htm
8. CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS (CCSDS) *Reference Model for an Open Archival Information System (OAIS), Blue Book*. (2002)
<http://public.ccsds.org/publications/archive/650x0b1.pdf>
9. CONVENIO DE BERNA PARA LA PROTECCIÓN DE LAS OBRAS LITERARIAS Y ARTÍSTICAS
<http://www.bibliotecasvirtuales.com/biblioteca/derechosdeautor/conveniodeberna.asp>
10. CORNELL UNIVERSITY LIBRARY. *Digital to Microfilm conversion: Demonstration project*. 1994-1996
<http://www.library.cornell.edu/preservation/com/comfin.html>



11. COUNCIL ON LIBRARY AND INFORMATION RESOURCES (CLIR). *Risk Management of digital information: A file format investigation*. 2000
<http://www.clir.org/pubs/reports/pub93/pub93.pdf>
12. IBM, *The UVC, a method for preserving documents*. 2002
http://www.kb.nl/hrd/dd/dd_onderzoek/reports/4-uvc.pdf
13. ICTU. *XML and Digital Preservation*. 2002
http://www.digitaleduurzaamheid.nl/bibliotheek/docs/white-paper_xml-en.pdf
14. IFLA e ICA para UNESCO. *Directrices para proyectos de digitalización de colecciones y fondos de dominio público, en particular para aquellos custodiados en bibliotecas y archivos*. 2002
http://travesia.mcu.es/documentos/pautas_digitalizacion.pdf
15. KEEFER, Alice; GALLART, Núria. *La preservación digital y las universidades: el estado de la cuestión*. 2003
<http://eprints.rclis.org/archive/00004816/>
16. KEEFER, Alice; GALLART, Núria. *La preservación de recursos digitales, El reto para las bibliotecas del siglo XXI*. Editorial UOC. 2007
17. LYNCH, Clifford. *Canonicalization: A fundamental tool to facilitate preservation and management of digital information*. 1999
<http://www.dlib.org/dlib/september99/09lynch.html>
18. MARCUM, Deanne. *Requirements for the Future Digital Library* (Traducción al español). 2003
<http://www.aab.es/pdfs/baab79/79a3.pdf>
19. RESEARCH LIBRARIES GROUP (RLG) Y COMMISSION ON PRESERVATION AND ACCESS (CPA). *Preserving Digital Information*. 1996
<http://www.oclc.org/programs/ourwork/past/digpresstudy/final-report.pdf>
20. ROBLEDANO ARILLO, Jesús. *Digitalización y gestión de imágenes digitales*. 2007
21. SILLÖ, Teresa. *Fundamentos tecnológicos del acceso abierto: Open Archives Initiative y Open Archival Information System*. 2005
<http://eprints.rclis.org/archive/00005887/01/EPITSilio.pdf>



22. UNESCO. *Carta para la preservación del Patrimonio Digital*. 2003
http://portal.unesco.org/ci/en/files/13367/10676067825Charter_es.pdf/Charter_es.pdf
23. UNESCO *Directrices para la Preservación del Patrimonio Digital*. prepared by the National Library of Australia. (2003)
http://www.imaginar.org/dppd/DPPD/0_DPPD.pdf (Traducido al español)
<http://unesdoc.unesco.org/images/0013/001300/130071e.pdf> (Original en inglés)
24. VERCELLI, Ariel. *La conquista silenciosa del ciberespacio, Creative Commons y el diseño de entornos digitales como nuevo arte regulativo de Internet*. 2004
<http://www.arielvercelli.org/lcsdc.pdf>

Serie Bibliotecología y Gestión de Información.

Títulos publicados 2009

Nº 43, Directrices para la creación de un Programa de Preservación Digital. Miguel Angel Rivera Donoso

Disponible en : <http://eprints.rclis.org>

NORMAS DE PUBLICACION

- **Objetivos**

La **Serie Bibliotecología y Gestión de Información** tiene por objetivo difundir la productividad, académica, las investigaciones y las experiencias de profesionales del área de la de Bibliotecología y Ciencia de la Información y del sector afin al mundo del libro y la lectura.

- **Alcance y política editorial**

Los trabajos a ser considerados en la Serie Bibliotecología y Gestión de Información, deben ser inéditos, no publicados en otras revistas o libros. Excepcionalmente el Comité Editorial podrá aceptar artículos que no cumplan con este requisito.

- **Arbitraje:** Los artículos recibidos serán sometidos a evaluación, a recomendación del Director de la Serie, donde el Comité Editorial enviará los trabajos a árbitros independientes para su aceptación o rechazo. En este último caso, se emitirá un informe al autor/a donde se señalen las razones de la decisión. El Comité Editorial podrá solicitar trabajos a autores de reconocido prestigio, quienes no serán sometidos al proceso de evaluación por árbitros.

- **Forma y preparación de manuscritos**

- **Extensión:** El artículo deberá tener una extensión entre 12 y 100 páginas, tamaño carta, espacio 1,5, cuerpo 12, incluidos gráficos, cuadros, diagramas, notas y referencias bibliográficas.

- **Idiomas:** Se aceptan trabajos en castellano, portugués e inglés, los cuales serán publicados en su idioma original.

- **Resumen y palabras claves:** El trabajo deberá tener un resumen en español e inglés en la primera página, de no más de 200 palabras, que sintetice sus propósitos y conclusiones más relevantes. De igual modo, deben incluirse tres palabras claves, que en lo posible no se encuentren en el título del trabajo, para efectos de indización bibliográfica.

- **Nota biográfica:** En la primera página, en nota al pie de página, deben consignarse una breve reseña curricular de los/as autores/as, considerando nacionalidad, título y/o grados académicos, desempeño y/o afiliación profesional actual y sus direcciones de correo electrónico, para posibles comunicaciones de los/las lectores/as con los autores/as.

- 
- **Referencia bibliográfica:** Utilizar para las referencias bibliográficas la modalidad de (Autor, año) en el texto, evitando su utilización a pie de página. Ejemplo: (González, 2006). Agregar al final del texto, la bibliografía completa. Sólo con los/las autores/as y obras citadas, numeradas y ordenadas alfabéticamente. Para el formato de la bibliografía, utilizar la “Guía para la presentación de referencias bibliográficas de publicaciones impresas y electrónicas” disponible en formato electrónico en :

<http://eprints.rclis.org/5163/1/ReferenciasBibliograficas.pdf>

- **Derechos:** Los derechos sobre los trabajos publicados, serán cedidos por los/as autores/as a la **Serie**.
- **Investigadores jóvenes:** El Comité Editorial considerará positivamente el envío de trabajos por parte de profesionales y/o investigadores/as jóvenes, como una forma de incentivo y apoyo a quienes comienzan su carrera en investigación.
- **Ejemplares de cortesía:** Los/as autores/as recibirán un ejemplar de cortesía del trabajo publicado.
- **Envío de manuscritos**
Todas las colaboraciones deberán ser enviadas impresas en duplicado. Los autores/as podrán remitir sus artículos en CD, o al correo electrónico: hector.gomez@utem.cl , en programa Word (office).