InterPARES 2 Project

International Research on Permanent Authentic Records in Electronic Systems

TEAM Mexico

Información para Contactos

En Canadá:

InterPARES Project
School of Library, Archival and Information Studies
The University of British Columbia
Vancouver, BC V6T 1Z3 Canada
TEL: +1 (604) 822-2694
FAX: +1 (604) 822-1200



Dr. Luciana Duranti, Project Director
+1 (604) 822-2587
luciana.duranti@ubc.ca

Randy Preston, Project Co-ordinator
+1 (604) 822-2694
interpares.project@ubc.ca

En México:
Juan Voutssas
CUIB - UNAM. Torre II de Humanidades. Piso 11
Cd. Universitaria. 04510, México, D.F.
voutssas@unam.mx (52)55 5623-0361

La mayor parte del financiamiento del Proyecto InterPARES proviene del *Consejo para la Investigación de las Ciencias Sociales y las Humanidades del Canadá*, La *Comisión Nacional para los Documentos de Archivo y Publicaciones Históricas* de los EUA y la *Fundación Nacional para la Ciencia* de los EUA. Fondos adicionales provienen de la Universidad de la Columbia Británica del Canadá a través del *Fondo para la Investigación Hampton*, El *Fondo Vicepresidencial para la Investigación y Desarrollo*, el Decano de Artes y la Escuela de Estudios de Bibliotecología, Archivología e Información.

Para mayor información véase el sitio *Web* del proyecto en:
http://www.interpares.org Existe un apartado especial del *"Team México"*

Gc

Guía del Creador Personal

CREACIÓN Y CONSERVACIÓN DE MATERIALES DIGITALES: LINEAMIENTOS PARA LOS INDIVIDUOS

Elementos de la Preservación

		5 Mg Migración	6 Pr Protección			
8 Md Metadatos	9 Re Respaldo	10 It Integridad	11 Ex Exactitud	12 Ff Forma Fija	13 Au Autenticidad	
		16 Io Interoperabilidad	17 Cn Conciencia	18 Ob Obsolescencia		20 Fx Fijeza
25 Tc Tercero confialan		26 Og Organización	27 Fb Fiabilidad		29 At Autenticación	30 Ce Contenido estable
			34 As Accesibilidad			37 Id Identidad

Traducción al español: Juan Voutssas - TEAM Mexico

Introducción

La mayor parte de la información es creada y almacenada hoy en día en forma digital. Las ventajas de los medios digitales les son familiares en la actualidad a todo mundo. Los documentos pueden ser creados, editados y revisados rápida y fácilmente. Gracias a la *Internet*, pueden ser distribuidos globalmente con la velocidad del relámpago; además, pueden ser manipulados en forma tal que son útiles para múltiples propósitos. El medio digital resuelve además los añejos problemas de almacenamiento asociados a grandes archivos en papel.

No obstante, las bendiciones de la era digital no vienen sin sus desventajas. Ha sido sólo hasta años recientes que las personas han comenzado a darse cuenta cabalmente de los problemas inherentes a los medios digitales. Por ejemplo, existe el hecho de que la información digital sólo puede ser accedida a través de un computador o dispositivo similar. Además, ese equipo debe contar con los programas adecuados para poder leer apropiadamente las *cadenas de bits* contenidas en su memoria. La facilidad de reproducción de documentos y la proliferación de sus copias dificulta la identificación de la versión completa o final de estos, y la facilidad de su distribución obstaculiza la preservación de los derechos de propiedad intelectual. Finalmente, todos los materiales digitales son vulnerables a la acción de virus informáticos o simples fallas tecnológicas y los rápidos cambios generacionales de equipos y programas los ponen en riesgo de quedar inaccesibles en corto plazo.

Con todos estos problemas, no es de extrañar que muchas personas añoren ya la cómoda tangibilidad del papel. Aún cuando nuestros sistemas de creación y conservación de información continuarán por algún tiempo como sistemas híbridos, –esto es, conformados por materiales tanto en papel como digitales– , obviamente no hay marcha atrás en el camino de la digitalización. En consecuencia, todos debemos hacer conciencia de los riesgos a los que se enfrentan los documentos digitales y además saber cómo minimizar de la mejor manera esos riesgos.

Estos lineamientos han sido desarrollados para aquellas personas que crean materiales digitales en el transcurso de sus actividades cotidianas profesionales y personales con el propósito de ayudarles a tomar decisiones informadas acerca de cómo crear y conservar esos materiales de formas que ayuden a asegurar su preservación durante todo el tiempo que sean requeridos. Los lineamientos también son útiles para pequeñas organizaciones o grupos de individuos tales como consultorios médicos, oficinas de consultores o equipos de investigadores en ciencias, artes o humanidades.

Estos lineamientos pueden ser aplicados a múltiples tipos de datos, documentos y publicaciones digitales, pero son en especial aplicables e importantes para documentos de archivo digitales. Estos documentos de archivo son aquellos que usted crea, recibe y usa en su quehacer cotidiano, y que conserva precisamente porque probablemente los necesitará el día de mañana, o porque desea dejar evidencia por escrito de lo que ha hecho. Por lo mismo, usted necesita ser especialmente cuidadoso en conservarlos y preservarlos. Estos lineamientos son una guía tanto para esos documentos que necesitan ser conservados por periodos cortos de tiempo como para aquellos que requieren de ser preservados a largo plazo. El apego a estos lineamientos coadyuvará a asegurar que esos documentos de archivo digitales que ameritan ser preservados por periodos largos en un repositorio archivístico digital continúen siendo accesibles hasta el momento en que se decidiese pasarlos al resguardo de un custodio permanente confiable.

Definiciones

Antes de presentar las recomendaciones guía para la creación y conservación de materiales digitales, es conveniente y útil clarificar el significado de algunos términos utilizados a lo largo de este documento.

Para fines de esta guía, un **documento de archivo** (en inglés: record) se define como un documento elaborado o recibido por una persona física o moral durante el curso de una actividad práctica –ya sea como instrumento o derivado de esa actividad– y que es separado (apartado, guardado) para acción posterior o como referencia. También se le conoce como "documento archivístico". Una **publicación** se define como un documento creado para ser diseminado o distribuido a un público a escala mayor. Todos los documentos de archivo y publicaciones son documentos que contienen datos. Un **documento** es información puesta sobre un soporte con una forma fija. La **información** es un conjunto de datos con propósito de ser comunicada a lo largo del tiempo y el espacio; finalmente **dato** es la pieza más pequeña e indivisible de información que tiene un significado.

El propósito de esta guía es el de proporcionar recomendaciones para la creación y conservación de materiales digitales en general, y específicamente documentos de archivo digitales que puedan seguir siendo conservados exactos y auténticos a lo largo del tiempo. Para facilitar su aplicación, debemos definir los términos "fiabilidad", "exactitud", "autenticidad" y "autenticación".

Para fines de esta guía, **fiabilidad** (reliability) es uno de los elementos que junto con *autenticidad* (authenticity) y *exactitud* (accuracy) conforman la *confianza* (trustworthiness) de un documento de archivo; la fiabilidad existe cuando un documento de archivo puede establecer, declarar o sostener al acto o hecho del que es relativo y es establecida determinando la competencia del autor, y examinando tanto la completitud en la forma del documento de archivo como el nivel de control ejercido durante su proceso de creación. La **exactitud** existe de acuerdo con el grado en el que datos, información, documentos o archivos son precisos, correctos, veraces, libres de errores o distorsiones, y pertinentes a un asunto o materia. Para asegurar la exactitud, es necesario ejercer control preciso sobre los procesos de creación, transmisión, conservación y preservación de los documentos de archivo. A lo largo del tiempo, la responsabilidad de la exactitud se traslada del autor al custodio de los documentos de archivo y finalmente -y en su caso- al preservador a largo plazo de los mismos. La **autenticidad** consiste en la acreditación de un documento de archivo de ser lo que pretende ser sin alteraciones o corrupciones. Los documentos auténticos son los que han mantenido su identidad e integridad al paso del tiempo gracias a la evidencia de su carácter, requisitos o circunstancias inherentes. Entra en riesgo cuando los documentos son transmitidos a lo largo de espacio y tiempo. A la larga, la responsabilidad de la autenticidad se traslada del custodio de los documentos de archivo al preservador a largo plazo de los mismos. **Autenticación** (authentication) consiste en la declaración de autenticidad de un documento de archivo en cierto punto específico del tiempo realizada por una persona con calidad jurídica y con autoridad para hacer tal declaración (p.ej. servidor público, notario, autoridad certificadora). Por lo mismo, es un medio para probar que los documentos de archivo son lo que pretenden ser en un momento dado. Las medidas externas de autenticación digital, como por ejemplo la adición de firmas digitales sólo pueden asegurar que los documentos de archivo son auténticos al momento de recibirse y no pueden ser repudiados entonces, pero tarde o temprano deberán ser migrados a otro formato y una vez transformados no puede asegurarse que estos continúan siendo auténticos después de ello.

1. Seleccione el equipo y programas de cómputo así como los formatos de archivo que aseguren la mayor probabilidad de que los materialesa digitales permanezcan accesibles a lo largo del tiempo.

El acceso a los materiales digitales depende de contar con los programas de cómputo adecuados. Aquellos programas que no son compatibles con versiones previas (compatibilidad retrospectiva) o con las versiones futuras (compatibilidad prospectiva) dificultarán a la larga el acceso de los documentos de archivo. Los programas o aplicaciones necesitan también interactuar apropiadamente con otros programas y sistemas (interoperabilidad). El prestar atención a los siguientes seis factores ayudará a asegurar que su equipo y programas de cómputo mantengan la accesibilidad a los materiales.

A. Seleccione aquellos programas que desplieguen los materiales como aparecieron originalmente. Idealmente, los materiales digitales deben conservar su apariencia exacta a lo largo del tiempo para ser totalmente inteligibles y accesibles. Asegúrese de que los nuevos programas sean capaces de leer sus materiales anteriores en el formato en el que han sido conservados y de que desplieguen de manera correcta en la pantalla en la misma forma documental en la que se veían originalmente. En otras palabras, los nuevos programas de cómputo deben ser compatibles con los anteriores.

B. Seleccione equipos y programas de cómputo que le permitan compartir los materiales digitales con facilidad. Los programas de cómputo deben ser capaces de poder dar salida a los materiales en diferentes formatos. A esta habilidad de interactuar fácilmente con otras plataformas tecnológicas se le conoce como **interoperabilidad**. Ello le facilitará acceder a sus materiales además de transferirlos hacia otros sistemas.

C. Seleccione programas de cómputo estándares. Esto es una de las mejores cosas que usted puede hacer para que sus materiales digitales duren. Los estándares avalados por organismos nacionales o internacionales son los mejores. A estos se les conoce como estándares ***de jure***. Si estos no existiesen para sus materiales, usted puede ayudar a asegurar la longevidad adoptando programas ampliamente aceptados y utilizados. A estos estándares se les conoce como estándares ***de facto***. Los programas de fuente abierta (open source) que son generalmente no propietarios, son altamente recomendados. (véase el apartado "G" en la siguiente página).

<< Estándar de Jure >>

Estándar emitido por algún organismo dedicado y/o autorizado para la emisión de ellos. Pueden ser nacionales (como NOM, ANSI), multinacionales (como CEN) o internacionales (como ISO). En formatos, dos estándares internacionales son PDF (estándar PDF para archivos) y ODF Formato OpenDocument de OASIS).

<< Estándar de Facto >>

Un estándar que no ha sido emitido por ningún organismo oficial dedicado a ello, sino más bien impuesto por el uso y aceptación generalizados por parte de una comunidad. Por ej., formatos de archivo tales como PDF, TIFF, DOC y ZIP.

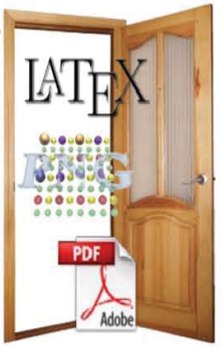
D. Conserve todas las especificaciones de los programas de cómputo. Este tipo de documentación (como los manuales de los sistemas, programas y otros materiales detallados similares) serán esenciales en un futuro para poder acceder a los materiales digitales o para migrarlos a nuevas plataformas según la tecnología vaya avanzando. Es particularmente importante documentar perfectamente los programas construidos por su propia organización.

E. Si usted hace adaptaciones particulares a programas de cómputo, asegúrese de documentar perfectamente los cambios que haga. Proporcione información detallada de todas las modificaciones y ajustes que usted realice y describa claramente las características y propiedades de los materiales digitales que esos cambios introducen y los objetivos que usted persigue con esas modificaciones. Una buena práctica es documentar esos cambios como comentarios intercalados en las líneas del código de la programación. Así la información no se perderá ya que forma parte del archivo en sí, y esto será muy útil a aquellos que deban hacer cambios al programa en un futuro según la tecnología avance.

F. Documente la construcción de su sistema de forma integral para ayudar a asegurar su accesibilidad.

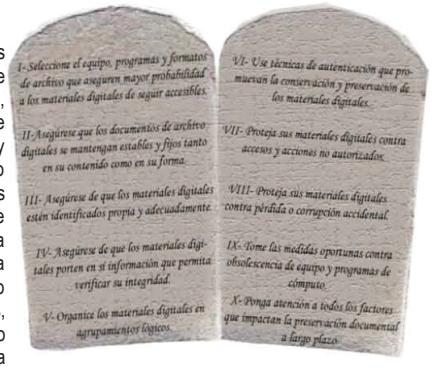
Usted debe documentar también la estructura y funcionalidad de sus sistemas. Esto significa identificar el equipo de cómputo, las especificaciones de sistemas operativos, programas, "paquetes" y bases de datos; los demás componentes, incluyendo periféricos. Esta información debe describir cómo es que los sistemas representan la información así como la forma en que la procesan y la comparten entre ellos y el usuario. Estas recomendaciones básicas aseguran que aquellos que vengan después de usted entiendan cabalmente todo el contexto en el que usted se desenvuelve hoy y proveerán la información necesaria para actualizar los sistemas cuando la tecnología evolucione.

G. Siempre que sea posible, prefiera formatos de amplio uso y aceptación, no propietarios, independientes de la plataforma, con compresión sin pérdida y con especificaciones ampliamente disponibles. A este tipo de formatos de archivo se les conoce también como "*formatos abiertos*" (open formats), lo cual significa que sus especificaciones de construcción han sido publicadas y están ampliamente disponibles y por tanto se les considera *"no propietarios"*. No obstante, esto también puede significar que está libre de patentes y de pago de derechos por su uso y/o que está ampliamente difundido y aceptado. Nótese que los formatos "abiertos" no necesariamente tienen que ser producidos por aquellas organizaciones que producen programas de fuente abierta o libre, (en los que los códigos fuente de los programas están disponibles para hacer cambios). Los programas de fuente abierta o libre no siempre producirán documentos en formatos "abiertos". Distinga usted bien entre formatos de archivo, formatos con envolturas (wrappers) o contenedores (containers), y formatos "etiquetados" (como archivos XML), y asegúrese de documentar bien las características de la versión, el encodificado, etcétera. En documentos XML, asegúrese de acompañar siempre a los documentos con su esquema o *"descriptor del tipo de documento"* (DTD) correspondientes. Si por alguna causa no es conveniente para usted seguir esta recomendación, consulte con archivos que preserven este tipo de información digital y seleccione de entre los formatos que esta organización recomiende para preservación digital a largo plazo. De preferencia, no aplique técnicas de compresión a sus materiales digitales; si decide hacerlo, aplique técnicas de compresión avaladas internacionalmente, como las denominadas técnicas de *"compresión sin pérdida"*.



Fj
Fijeza

2. Asegúrese de que los materiales digitales conservados como documentos de archivo digitales permanezcan estables y fijos, tanto en su contenido como en su forma.



Una de las grande ventajas de los materiales digitales es la enorme facilidad con la que la información puede ser editada, revisada o actualizada. Pero ello también significa que información importante puede ser modificada, dañada y hasta destruída, ya sea por accidente o a propósito. Esto es un problema particularmentre importante para los documentos de archivo, ya que se supone que una de sus características inherentes es que su contenido sea inmodificable y que no haya sido cambiado. Esto implica que los datos e información del documento de archivo no pueden ser sobreescritos, alterados, borrados o adicionados. Todo sistema que contenga datos o información que fluyen y están siempre cambiantes en realidad no contienen documentos de archivo hasta que alguien decide construirlos y salvarlos con una **forma fija** y un **contenido estable**.

<< Fijeza >>

La cualidad de un documento de archivo que asegura su forma fija y contenido estable.

Mientras que la idea de contenido estable es bastante simple, el concepto de forma fija es bastante más complejo. Esencialmente, significa que el mensaje expresado o contenido en un documento de archivo digital (o cualquier otro objeto digital) puede ser representado (rendered) en la misma forma documental que tenía en la pantalla la primera vez que fue recibido y salvado. Por tanto, la *"cadena de bits"* (bitstream) que conforma al documento de archivo digital y define su representación digital (esto es, su formato de archivo) puede cambiar, pero su representación documental no puede, no debe hacerlo. Un ejemplo sencillo de esto sucede cuando un documento elaborado en el formato .doc de Microsoft Word es salvado en el formato .pdf de Adobe, –la representación documental del documento, también llamada su **forma documental**– no ha cambiado aunque su formato sí lo haya hecho, y por tanto podemos afirmar que el documento tiene una forma fija.

<< Forma Fija >>

La cualidad de un documento de archivo que asegura que la apariencia documental o presentación sea la misma cada vez que el documento es recuperado.

<< Contenido Estable >>

La cualidad de un documento de archivo que hace inmutables a los datos e información contenidos en él, y requiere acciones específicas para agregar una actualización o crear una nueva versión.

En algunos casos, los materiales digitales pueden ser presentados de variadas formas, –en otras palabras, la información que ellos expresan puede manifestarse de varias formas documentales–; por ejemplo, ciertos datos estadísticos pueden ser presentados en forma de gráfica de "pastel", gráfica de barras o en forma de tabla. De cualquier forma, las variaciones a las presentaciones están generalmente limitadas por el propio sistema. En estos casos, decimos que cada representación documental tiene su forma fija y contenido estable, ya que la información es seleccionada de un repositorio fijo estable dentro del sistema y las reglas del mismo gobiernan y delimitan las posibles formas de sus representaciones documentales.

Una situación similar ocurre cuando la selección de contenido y forma proviene de un gran repositorio de información fija la cual es parcialmente accedida cuando se efectúa una consulta (query) sobre el sistema. Si la misma consulta siempre produce la misma salida en contenido y forma documental, se considera que esta salida tiene forma fija y contenido estable. Por tanto, si usted, –como autor del documento de archivo–, preestablece reglas fijas para la selección de su contenido y su forma documental, de tal forma que exista sólo un cierto número estable y finito de variabilidad de ellas, esto quiere decir que el documento tiene **variabilidad vinculada** (acotada o limitada), y usted puede afirmar que el documento tiene forma fija y contenido estable.

Fj
Fijeza

<< Variabilidad Vinculada >>
(Acotada, Limitada)

La cualidad de un documento de archivo que asegura que sus presentaciones documentales y los cambios a su forma, contenido y/o composición están limitados y controlados por reglas fijas, de tal forma que la misma pregunta, solicitud o interacción (query) siempre genera el mismo resultado.

La preocupación por la representación documental de los materiales digitales es particularmente importante para conservar y valorar la fiabilidad y exactitud de los documentos de archivo. Las futuras actualizaciones, conversiones o migraciones de datos podrían desembocar en cambios a la forma documental; por tanto, será muy pertinente que usted establezca de entrada la forma documental de los documentos de archivo que van asociados a cada actividad o procedimiento de la organización e identifique sus características esenciales, –esto es, los elementos **extrínsecos** e **intrínsecos** esenciales–, de cada representación o forma documental. Esto le advertirá a usted en un futuro acerca de si cierto cambio en un documento de archivo implicará pérdida de su identidad o integridad, muy especialmente si usted se mueve en la esfera del "arte digital", en donde una descripción certificada de esas características esenciales por parte del artista ayudaría a reconocer e identificar los derechos de propiedad intelectual ligados a una obra así descrita.

<< Forma Documental >>

Reglas de representación según las cuales el contenido de un documento de archivo, sus contextos administrativo y documental así como su autoridad son comunicados. La forma documental posee tanto elementos extrínsecos como intrínsecos.

<< Elemento Extrínseco >>

Elemento de la forma documental de un documento de archivo que forma parte de su apariencia externa. Entre los tipos de elementos extrínsecos se encuentran rasgos de presentación (como fuentes tipográficas), hipervínculos, firmas electrónicas, sellos electrónicos, sellos digitales de tiempo emitidos por un tercero de confianza y signos especiales (marcas de agua electrónicas, etc.).

<< Elemento Intrínseco >>

Elemento de la forma documental de un documento de archivo que forma parte de su composición interna y que expresa su contexto inmediato. Incluye nombres de los involucrados en su creación, acción o materia de la que trata, fechas de creación, transmisión, etc.

Id
Identidad

3. Asegúrese de que los materiales digitales estén propiamente identificados.

El proporcionar un nombre con significado a un archivo dentro de la computadora ayuda a identificar su contenido además de facilitar su localización, pero debemos estar conscientes de que el identificar plenamente a los documentos de archivo va más allá del simple nombrado de sus archivos. La identificación plena sirve para diferenciar a un documento de archivo de otro, para distinguir entre distintas versiones del mismo documento y para proveer evidencia de la identidad de un documento de archivo desde el momento de su creación hasta el de su preservación a largo plazo.

A la información acerca de materiales digitales que sostiene su identificación y recuperación se le conoce como "**metadatos**". La mayoría de las aplicaciones de cómputo que manejan información automáticamente "etiquetan" a los materiales digitales con ciertos datos que permiten establecer su identidad ya que ese tipo de información es necesaria para poder localizarlos efectivamente. Sin los metadatos, sería prácticamente imposible encontrar un documento sin abrir y leer a lo largo de carpetas y subdirectorios. Además, los metadatos describen las propiedades y atributos de los materiales digitales, características que son necesarias para evaluar su autenticidad; de ahí la importancia de asegurarse de que todas las propiedades y atributos esenciales sean registrados correctamente.

<< IDENTIDAD >>

El conjunto de características inherentes a un documento de archivo que lo identifican de forma única y lo distinguen de otros documentos de archivo. Junto con integridad, conforma la autenticidad de un documento.

A las propiedades y atributos que manifiestan la identidad de los materiales digitales se les conoce como **metadatos de identidad**; éstos incluyen:

A. Nombres de las personas involucradas con la creación de los materiales digitales. Estos incluyen:

- **autor** – persona física o jurídica que tiene la autoridad y capacidad para emitir un documento de archivo o en cuyo nombre u orden el documento de archivo ha sido emitido.
- **escritor** – persona física o puesto responsable de articular el contenido de un documento de archivo.
- **originador** – persona física, jurídica o puesto responsable de la cuenta electrónica o ambiente tecnológico donde los materiales son creados o desde donde son transmitidos (este dato es relevante cuando ni el autor ni el escritor son las personas responsables de crear y/o transmitir el documento). Un ejemplo de ello es un correo electrónico cuyo remitente sea una persona y tenga un documento adjunto de otro autor.
- **destinatario** – persona física o jurídica a quien se dirige o para quien está previsto un documento de archivo.
- **receptor** – persona física o jurídica a quien se le envía copia del material, incluyendo copia ciega.

B. Nombre de la acción, materia o asunto. El título o materia de la que trata el material digital.

Id
Identidad

C. Forma documental. Estas incluyen: reportes, cartas, contratos, tablas, listas, etcétera.

D. Representación digital. Estas incluyen: formato, envoltura, codificación, etcétera.

E. Fecha(s) de creación y tranmisión. Estas incluyen:

- **fecha cronológica** escrita en los materiales o en la cual los materiales fueron compilados;
- **fecha de transmisión y/o recepción**; y
- **fecha de archivado**; esto es, la fecha cuando los materiales fueron asociados a una carpeta o directorio de computadora, u a otro esquema de clasificación o plan de archivado (Véase recomendación 5).

F. Expresión del contexto documental. Estas incluyen: código de clasificación, o el nombre del subdirectorio o archivo de computadora, o número de clasificación, o nombre del gran grupo de documentos de archivo al cual pertenece este material digital (Véase recomendación 5).

G. Indicación de anexos al documento, cuando aplique.

H. Indicación de los derechos de autor o de propiedad intelectual, cuando aplique.

I. Indicación de la presencia o remoción de firma digital, cuando aplique (Véase recomendación 6, sección de autenticación dependiente de la tecnología).

J. Indicación de otras formas de autenticación, cuando aplique. Esto podría incluir, por ejemplo, la presencia de una **corroboración**, (esto es, una mención específica de los medios usados para validar el documento de archivo), un **testimonio** (esto es, la validación de un documento de archivo por parte de aquellos que intervinieron en su confección, o testificaron la acción o firmaron el documento de archivo), una **suscripción**, (esto es, el nombre de un autor o escritor quien suscribe el documento al pie del mismo), o una **calificación o firma,** (esto es, la mención del título, capacidad, autoridad, cargo y/o dirección de la o las personas que firman el documento de archivo).

K. Indicación de borrador o del número de la versión del documento, cuando aplique.

L. Existencia y localización de materiales duplicados fuera del sistema digital, cuando aplique.

Cuando existan múltiples copias de un documento digital, usted debe indicar cuál es la **copia oficial o autorizada**. Si el documento ha sido certificado por el autor como "reproducción aprobada" de una obra (por ejemplo, una obra de arte digital) se requiere el indicio de la existencia de tal certificado. Si el documento abarca material amparado por derechos de autor, el indicio de la autorización correspondiente, (o la razón por la cual no existe), debe ser registrado junto con las fechas asociadas.

<< COPIA AUTORIZADA >>

La instanciación de un documento de archivo considerada por su creador como el documento oficial y que ha sido sujeta a controles procedimentales por lo general no requeridos por otras instanciaciones.

It
Integridad

4. Asegúrese de que los materiales digitales porten información que ayude a verificar su integridad.

Los metadatos de identidad permiten distinguir un material digital de otro; a diferencia de estos, los **metadatos de integridad** son aquellos que permiten al usuario inferir que el material digital es el mismo que cuando fue creado. Nótese que estos metadatos no implican verificación o demostración de ese hecho, ya que ello requiere de la comparación de una copia dada con otra resguardada en otro lugar. Los materiales digitales tienen **integridad** si están intactos e incorruptos, esto es, si los mensajes que portaban para comunicar o lograr su propósito permanecen inalterados. Ello significa que la integridad física de los materiales, tal como la cadena de bits que porta el mensaje ha podido ser alterada, siempre y cuando la articulación de su contenido y los elementos necesarios de su forma documental permanezcan iguales (Véase recomendación 2). El contenido y los datos en ellos pueden considerarse inalterados si son idénticos en valor y presentación (estos es, su forma y lugar en la pantalla) al contenido y datos que fueron salvados al momento de la primera manifestación del documento. Los atributos que describen la integridad de los materiales digitales tienen relación con la conservación o mantenimiento de los materiales, e incluyen la responsabilidad de su manejo apropiado, de la supervisión y la documentación de las transformaciones tecnológicas o transferencia de los materiales a otros sistemas. Los metadatos de integridad incluyen:

<< INTEGRIDAD >>

La cualidad de un documento de archivo de estar completo e inalterado en todos sus aspectos esenciales. Junto con identidad, conforma la autenticidad de un documento.

A. Nombre(s) de la persona o dependencia. La persona, puesto, dependencia u oficina que usa el material digital para realizar sus tareas y/o responsabilidades.

B. Nombre(s) de la persona o dependencia que tienen la responsabilidad primaria del resguardo de los materiales. Pueden ser los mismos que los del inciso anterior o pueden ser diferentes.

C. Indicación de las anotaciones agregadas a los materiales digitales. Cuando aplique.

D Indicaciones de los cambios tecnológicos a los materiales o a los programas utilizados para la administración y acceso a los materiales. Por ejemplo, cambios en la codificación, envolturas o formatos; actualizaciones de versiones de los programas, conversiones de diversos componentes digitales vinculados al material, integraciones de varios componentes digitales en uno sólo (audio, video, texto, fuentes, etcétera).

E. Código de restricciones al acceso. Indicación de las personas o puestos autorizados para leer el material, cuando aplique.

F. Código de privilegios de acceso. Indicación de las personas o puestos autorizados para agregar anotaciones al material o borrarlos del sistema, cuando aplique.

G. Código de "registro vital". Indicación del grado de importancia de documento de archivo para la continuidad de las actividades para las que fue creado, cuando aplique. Este dato existe generalmente en ciertas comunidades críticas, como ambientes legales o médicos, donde el documento no debe ser borrado nunca.

H. Disposición o borrado planeado. Remoción del material establecida previamente; por ejemplo: desde estado activo a inactivo, transferencia a otro sistema o a un custodio confiable, etc. (Véase la recomendación 10).

Or
Organización

5. Organice los materiales digitales en agrupamientos lógicos.

La administración y recuperación de sus materiales digitales puede ser optimizada si usted puede acomodarlos en conjuntos de cierto volumen, en lugar de uno por uno. De allí la importancia de que usted agrupe sus materiales digitales de alguna manera lógica. La categorización escogida puede ser el reflejo de la manera en que usted trabaja cotidianamente, sus actividades, procedimientos, áreas temáticas, o alguna otra clase de organización estructural. Separar sus documentos de archivo de sus materiales digitales es un importante primer paso. La organización de sus documentos de archivo puede estar basada en en los diferentes tipos de ellos o en el periodo de tiempo por el que ciertas clases de documentos requieran estar resguardados. Tales agrupamientos pueden interrelacionarse entre ellos de forma simple o jerarquizada, según mejor convenga a sus necesidades. Generalmente, la estructura debería ser consistente con la que la organización usaría en el caso de archivos en papel u otros medios semejantes, de tal forma que los documentos del mismo tipo o relacionados con la misma actividad, tema o persona, puedan ser fácilmente identificados y recuperados como parte de un agrupamiento conceptual, -un "expediente"-, según se necesite.

<<ESQUEMA DE CLASIFICACIÓN>>

Un plan o esquema para la identificación sistemática e información descriptiva de documentos de archivo así como las actividades de una organización en categorías basada en convenciones de estructura lógica, métodos y reglas procedimentales.

(Véase también la recomendación 3)

El esquema de su organización debe ser también registrado en un documento que describa todos los agrupamientos de materiales existentes, así como sus interrelaciones. En este documento, el cual es llamado **esquema de clasificación** o plan de archivo, a cada grupo de documentos le es asignado un código o nombre que deberá ser asociado a cada documento de archivo del agrupamiento, sin importar su medio o ubicación. En consecuencia, todos los doumentos de archivo de un mismo grupo compartirán ese código o nombre, seguido de un número que indique su secuencia dentro del grupo. Este identificador debe ser registrado en los **metadatos de identidad** de sus documentos de archivo digitales así como en la carátula de sus documentos de archivo en papel, y debe ser único para cada documento.

<< METADATOS DE IDENTIDAD >>

Las propiedades o atributos que conforman la identidad de un objeto digital que debe ser resguardado como un documento de archivo.

(Véase también la recomendación 3)

El identificar la manera en que los grandes agrupamientos de documentos de archivo deben ser conservados facilitará su administración durante el tiempo que estos sean regularmente requeridos y ayudará a asegurar que los documentos que ameriten preservación a largo plazo sean marcados oportunamente y gocen de la protección adecuada que asegure su permanencia. A usted se le facilitará más y le resultará más eficiente asignar los periodos de retención, -esto es, el tiempo que usted requiere de guardar ciertos materiales-, a grupos de materiales que a documentos sueltos. El tratar de asegurar que ciertos materiales se conserven todo el tiempo que sea necesario deshaciéndose al mismo tiempo de lo que no es requerido puede volverse una tarea chocante e ineficiente pretendiendo hacerlo a nivel de documento por documento. Si usted establece que dentro de un agrupamiento algunos documentos deben permanecer más que otros usted podrá ahorrar tiempo al examinarlos en conjunto como grupo. Además, usted siempre puede crear subgrupos dentro de los agrupamientos que le faciliten aún más esta tarea durante el periodo de retención.

Au
Autenticación

6. Use técnicas de autenticación que aprovechen e impulsen la conservación y preservación de los materiales digitales.

La autenticidad de los materiales digitales se ve amenazada siempre que estos son transmitidos en el espacio (cuando son enviados a un destinatario o en las etapas donde viajan entre los programas) o en el tiempo (cuando están almacenados o cuando los equipos o programas usados para su proceso, almacenamiento o transmisión son actualizados o reemplazados). Dado que el hecho de separar o apartar los materiales digitales para futura acción o referencia para luego recuperarlos implica inevitablemente su desplazamiento a través de fronteras tecnológicas (desde los dispositivos de almacenamiento hasta los dispositivos de despliegue). Por lo mismo, la inferencia de la autenticidad de los materiales digitales debe ser apoyada más adelante por evidencia de que estos han sido conservados usando tecnologías y procedimientos administrativos que garantizan su continua identidad e integridad o al menos minimizan los riesgos de alteración desde el momento en que los documentos de archivo fueron seleccionados originalmente hasta el punto en el que fueron subsecuentemente accedidos.

<< AUTENTICACIÓN >>

Declaración de autenticidad de un documento de archivo en cierto punto específico del tiempo realizada por una persona con calidad jurídica y con autoridad para hacer tal declaración (p.ej. servidor público, notario, autoridad certificadora).

Autenticación independiente de la tecnología.

Presunción de Autenticidad. Esta es una inferencia que se extrae de hechos establecidos y conocidos acerca de la manera en la que un documento fue creado y conservado. La adopción y aplicación consistente de las recomendaciones presentadas en este documento proveerán la mejor evidencia para apoyar esta presunción. Además, las recomendaciones son acumulativas: en la medida en que un mayor número de ellas sea satisfecho, y entre mayor sea el grado alcanzado en el llenado de cada una de sus especificaciones, más sólida será la presunción de autenticidad. La implementación exitosa de las recomendaciones aquí presentadas se logra al establecer y aplicar ininterrumpidamente políticas y procedimientos efectivos (Véase al final de este documento la referencia a los Recursos del Proyecto de Preservación InterPARES, inciso 3, *"Marco de referencia de Políticas"*). En un plano ideal, usted debe procurar implementar técnicas de autenticación apoyadas por procedimientos y políticas de administración documental que sean tan independientes y neutrales de la tecnología como sea posible.

Autenticación dependiente de la tecnología.

Existen técnicas de autenticación documental que son derivadas directamente de la tecnología y por tanto dependientes de ella; tal es el caso de las técnicas criptográficas digitales, como por ejemplo el agregar firmas, sellos o marcas de agua digitales a los documentos transmitidos y almacenados para garantizar su autenticidad. Estas técnicas tienen ya inclusive total valor legal en muchos países y organismos.

¡Precaución! Las firmas digitales están sujetas a obsolescencia tecnológica y en virtud de su propósito y funcionalidad intrínseca, su migración o actualización a nuevas versiones de programas puede resultar sumamente difícil. De hecho, el lapso de vida de las firmas digitales y otras técnicas afines puede llegar a ser más corto que el periodo de retención que cierto documento que debe ser conservado, debido a la rápida obsolescencia de las tecnologías relacionadas con las firmas. A menos que desarrollos futuros de las firmas electrónicas contemplen la forma de que estas puedan ser preservadas a lo largo de sucesivas plataformas tecnológicas, al momento de recibir un documento para preservación de largo plazo, el preservador debe considerar la posibilidad de desechar la firma digital del documento cuando esto sea posible, después de ser verificada.

Pr
Protección

7. Proteja sus materiales digitales contra accesos y acciones no autorizadas.

La exactitud y autenticidad de los materiales digitales no puede ser asumida nunca si existe una posibilidad de modificarlos sin dejar traza de ello. Usted debe ser capaz de poder demostrar que es imposible acceder o manipular los documentos sin ser identificado previa y posteriormente a la acción. La protección incluye el establecimiento de políticas de seguridad informática, acceso restringido a las instalaciones que guardan los documentos y acceso restringido a los sistemas, programas. equipos, redes y documentos, tanto para el personal interno de la organización como para los usuarios. Existen variadas técnicas para lograr esto que deberán ser exploradas por el preservador, como por ejemplo contraseñas, biométricos, "tokens", etcétera.

Es de suma importancia establecer una estructura de permisos o privilegios de acceso para todos los usuarios del sistema, (Véase la argumentación de los **metadatos de integridad** en la **recomendación 4**). Ahí se establecen los requerimientos para que ciertas personas tengan permiso o no para ver los documentos, modificarlos, borrarlos, descargarlos o transferirlos. En todo caso, debe ser imposible modificar un documento de archivo una vez que este ha sido completado y salvado de acuerdo con el **cuadro o esquema de clasificación** o *plan de archivo* establecidos. (Véanse las **recomendaciones 3 y 5**). Sólo la o las personas que tienen la responsabilidad expresa de la gestión de los documentos de archivo (recordkeeping) y la conservación documental deben poder ser capaces de modificar, borrar o transferir materiales del sistema. Además, este debe guardar bitácoras y trazas que permitan auditar claramente los accesos y acciones a los materiales para control de los privilegios de acceso.

Esta recomendación puede ser difícil de implementar en organizaciones donde ciertos funcionarios deben trabajar desde sus hogares, o en oficinas o comunidades pequeñas donde los empleados son muchas veces multifuncionales. Pero es de suma importancia recordar que si usted no puede demostrar que ha sido imposible para cualquiera acceder y/o manipular los materiales digitales sin haber sido identificado, la aseveración acerca de que sus documentos de archivo son *de facto* exactos y auténticos se vuelve irrelevante e intrascendente. En este sentido, puede ser útil conservar copias de al menos los documentos más relevantes fuera del sistema y establecer una rutina de comparación aleatoria entre ellos de forma periódica.

Re
Respaldo

8. Proteja sus materiales digitales contra corrupción o pérdida accidental.

Las computadoras no son a prueba de fallas; derivado de su uso, existe un sinnúmero de factores que pueden provocar corrupción o pérdida accidental de datos o documentos de archivo. La mejor forma de asegurarse contra estos accidentes es realizar copias de los documentos frecuente y periódicamente. Si además guardamos copias adicionales en ubicaciones remotas a nuestra organización, lograremos protección adicional contra desastres tales como fuego, robo, inundación, etcétera. Existen variadas técnicas de respaldo, programas y servicios de terceros al efecto. Existen inclusive versiones que generan y transmiten de forma autómatica los respaldos a sitios seguros.

A. Desarrolle una política rigurosa que asegure que su sistema es respaldado diariamente.

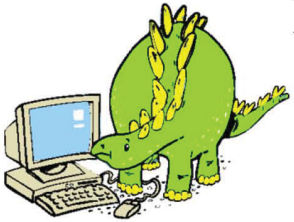
Su sistema es tan bueno como su último respaldo; por lo mismo, usted debe asegurarse de que sea respaldado con frecuencia; al menos una vez al día, usando métodos comprobados que garanticen que en caso de que algo vaya mal, usted y su organización podrán recuperar su información íntegra y rápidamente. Los respaldos realizados periódicamente deben "rotar" un juego de soportes o medios para asegurar que se cuenta con varias copias de los datos además de que las versiones más antiguas se destruyen al reescribir sobre ellos. Se recomienda tener respaldos actualizados de sistemas operativos y programas de cómputo además de los materiales digitales. Además de los respaldos cotidianos, es indispensable contar con un **"respaldo de emergencia"** en donde se encuentren todos los materiales digitales resguardados en computadores, soportes o medios ubicados en locaciones remotas externas a nuestra organización.

B. Seleccione e instale la mejor tecnología de respaldo de acuerdo con su contexto.

Estudie la tecnología y servicios de respaldo que estén disponibles y seeleccione aquellos que respondan mejor a las necesidades del contexto y características de su organización. Existen variadas posibilidades para ello, desde las acciones llevadas a cabo por una persona encargada de esta responsabilidad, hasta sistemas totalmente automáticos y redundantes que pueden respaldar inclusive enormes sistemas. El sistema de respaldo debe incluir una bitácora auditable, para que en caso de una falla del sistema de datos usted sepa desde cuándo debe recuperar datos y documentos a partir de los sistemas de respaldo.

Ob
Obsolescencia

9. Tome acciones contra la obsolescencia de equipo y programas de cómputo.



La velocidad a la que el equipo y programas de cómputo se vuelven obsoletos impone severos retos a la conservación y por tanto a la preservación a largo plazo de los materiales digitales. Una estrategia probada para contender con este problema es transferir ciertas funcionalidades desde los equipos de cómputo hacia los programas eliminando así la dependencia del equipo. Ello provee una manera más estable de conservar la función cuando el equipo se vuelva obsoleto.

Este ambiente tecnológico siempre cambiante significa que tanto las personas como las organizaciones deben actualizar regularmente sus sistemas digitales y los documentos de archivo en ellos contenidos, además de aquellos documentos que hayan sido transferidos a otros soportes tales como CD's, DVD's o cintas. Dicho de otra forma, cuando usted se percate de que ciertas partes del entorno tecnológico se están volviendo obsoletas, es conveniente que usted las vaya migrando a tecnologías actuales de acuerdo con sus requerimientos y posibilidades; de la misma forma, los materiales digitales relacionados con ellas también deben ser migrados a soportes con tecnologías actuales. Cuando se remplace cierto equipo, es importante verificar que el nuevo tenga capacidades que cubran perfectamente las del equipo anterior. Por ejemplo, un monitor nuevo debe poder desplegar a un documento que tenga elementos gráficos exactamente de la misma forma en que el monitor anterior lo hacía en lo tocante a su forma documental. La planeación correcta de sustituciones de partes de la plataforma tecnológica en forma gradual anualmente le permitirá a usted garantizar que esta no se vuelva obsoleta de golpe al mismo tiempo que no le impone gastos muy fuertes al tener que sustituir todo de una sóla vez.

En ciertas ocasiones sucede que es necesario conservar documentos de archivo por periodos largos en sistemas que se han vuelto obsoletos, aunque sucede con frecuencia que estos no deban ser consultados a menudo. Si esos documentos son de tipo textual y deben ser accedidos en forma secuencial -no aletatoria- es conveniente convertirlos de su forma digital a microfilme por medio de la tecnología llamada COM (computer output microfiche o salida de computador a microficha). Esta acción las protegerá contra pérdida o corrupción accidental mejor que cualquier otra forma. Otra medida protectora adecuada consiste en obtener una segunda copia y mejor aún una tercera de los documentos de archivo, y guardar estas en otra computadora o juego de discos o cintas en ubicaciones fuera de la sede de nuestros archivos. Al momento de remover documentos de archivo u otros materiales digitales de un sistema para transferirlos a otros soportes fuera del mismo es importante remover también sus metadatos correspondientes pero sin olvidar de agregarlos a los documentos transferidos documentando la operación. Para mayor detalle de la documentación necesaria en este aspecto, véase el **requerimiento 1**, en los apartados "D", "E", y "F".

Cn
Conciencia

10. Considere todos los factores relacionados con la preservación a largo plazo.

El enfoque de este documento ha estado alrededor de la creación y conservación temporal de toda clase de materiales digitales por parte de sus creadores y por todo el lapso que estos son requeridos por ellos, pero es importante pensar también en aquellos documentos que deberán ser preservados por largo plazo. Por lo general sólo una parte de los documentos que se conservan -aquellos considerados importantes- deberán ser preservados a largo plazo, pero es poco frecuente que las personas y las organizaciones pequeñas tengan la capacidad y la voluntad de proporcionar cuidado ininterrumpido y permanente a sus materiales digitales. Existen costos reales, -tanto económicos como humanos- involucrados en la preservación de documentos de archivo digitales, pero es necesario estar conscientes de que estas acciones son indispensables para la preservación de nuestro patrimonio documental digital, para la continuidad de los negocios y organizaciones y para la toma de decisiones fundamentadas.

Para iniciar este proceso y en un caso ideal, usted debe identificar a alguien que esté en posibilidad y deseo de hacerse cargo de sus materiales digitales una vez que estos ya no son requeridos en una base frecuente. Esta persona toma el papel de un "**custodio de confianza**". Éste consiste en un profesional -o grupo de ellos- pertenecientes a una organización -archivo o sociedad histórica- con capacidad y habilidades profesionales probadas para la gestión documental y su preservación y quien no tiene un interés o beneficio particular en la alteración de los documentos de archivo. En el caso de organizaciones u oficinas pequeñas, esta persona puede ser la que normalmente está encargada de administrar los documentos, organizarlos y archivarlos para su utilización cotidiana y a corto plazo. En el caso de individuos que tienen que administrar sus propios archivos digitales, esta tarea puede cederse a un profesional de archivos o bibliotecas, y en último caso uno mismo, asumiendo los costos y tareas de la preservación a largo plazo. En todos los casos, es indispensable trazar una estrategia de preservación desde el principio, ya que los materiales digitales que no han sido detectados y marcados para preservación digital y por tanto conservados bajo esa base de forma proactiva y apropiada, entran en riesgo inmediatamente. El apego estricto y cercano a estos lineamientos mejorará sin duda las posibilidades de su preservación.

<< Custodio de Confianza >>

Un preservador que puede demostrar que no tiene razón o interés alguno para alterar los documentos de archivo preservados ni permitir que otros lo hagan, y que es capaz de implementar todos los requerimientos necesarios para la preservación de copias auténticas de los documentos bajo su cuidado.

Conclusión.

Co
Conclusión

Este documento ha descrito una serie de actividades para individuos y pequeñas organizaciones con el propósito de crear y conservar materiales digitales de forma auténtica, exacta y fiable. Para todos ellos la tarea puede parecer difícil y tediosa, pero la alternativa es la posibilidad de que sus documentos digitales se corrompan, se pierdan y queden incompletos o inútiles a largo plazo. Las pequeñas organizaciones u oficinas se beneficiarán grandemente de especificar con claridad quién es la persona o personas responsables de velar por la conservación de sus materiales digitales. Tenga usted presente que no es necesario implementar todas y cada una de las recomendaciones descritas en esta guía en cada ocasión. Usted debe seleccionar aquellas que se adaptan a sus necesidades y contexto particulares. Habrá ocasiones en las que deberán considerarse medidas adicionales a las aquí descritas por causa de disposiciones legales o regulatorias de su campo, o debido a características propias de su actividad y en consecuencia de los documentos por ella producidos. En estos casos es recomendable siempre acudir al consejo de expertos en la materia; ello puede obtenerse en organizaciones de archivos municipales, estatales o nacionales, así como en las asociaciones profesionales de este tipo de personas. Esto es siempre benéfico y por tanto recomendable, y ayudará enormemente a las personas, pequeñas organizaciones y oficinas en la conceptualización de sus estrategias y medidas tendientes a la creación y conservación adecuada de sus documentos de archivo digitales.

El Proyecto InterPARES

La sociedad preserva su memoria en su arte y su arquitectura, en sus libros y otros impresos, y en las huellas que deja de sus esfuerzos y quehaceres capturados en sus documentos de archivo. Estos son documentos únicos ya que son partícipes de los resultados de las actividades de personas y organizaciones constituyéndose en la fuente primaria de conocimiento acerca de esas actividades. Los documentos de archivo se están generando cada vez más en formatos digitales lo cual dificulta su preservación debido a la rápida obsolescencia de equipos y programas de cómputo, la fragilidad de los medios de almacenamiento digital y la facilidad con la que este tipo de información puede ser manipulada. Una buena parte de la memoria documental de nuestra sociedad creada en forma digital ya ha sido amenazada y hoy en día es difícil cuantificar cuánta de esta información se ha perdido y cuánta de ella ha sido puesta a buen resguardo y a qué costo; lo que sí es seguro es que la amenaza es real y está ya dispersa por todas partes. Además, al momento de contender con ella debemos tener siempre presente que aunque la información sea preservada, de nada servirá si no podemos garantizar al mismo tiempo su autenticidad; es decir, su valor como fuente documental cierta. Por siglos, la autenticidad de los documentos de archivo estuvo basada en las firmas y sellos, en los mecanismos de control utilizados para su creación, transferencia conservación y uso así como en una cadena ininterrumpida de custodia sobre ellos. El uso de tecnología digital para la creación de documentos de archivo ha reconfigurado radicalmente a los elementos de forma tradicionales mediante los cuales estos documentos eran reconocidos como auténticos, ha trastornado los procedimientos de control y ha diluído el concepto de custodia física.

El *Proyecto internacional Para la Investigación Acerca de Documentos de Archivo Auténticos y Permanentes en Sistemas Electrónicos* -InterPARES o International Research on Permanent Authentic Records in Electronic Systems- fue iniciado en 1999 precisamente para contender contra estos factores. Este proyecto multidisciplinario concluyó sus investigaciones en 2006 e involucró a más de 100 investigadores de 20 países de los cinco continentes desarrollándose en dos etapas:

InterPARES 1 (1999-2001) se llevó a cabo bajo el enfoque de los preservadores y desarrolló investigación original acerca de la preservación de documentos de archivo administrativos creados y mantenidos en bases de datos y sistemas de gestión documental los cuales no eran ya necesarios para su creador para la realización de sus tareas cotidianas.

InterPARES 2 (2001-2006) se llevó a cabo bajo el enfoque del creador de los documentos de archivo con el propósito de desarrollar teoría capaces de asegurar la fiabilidad, exactitud y autenticidad de los documentos de archivo desde su creación y hasta su preservación. El enfoque del proyecto estuvo en documentos de archivo complejos, que son los típicamente creados en los sistemas interactivos, experienciales y dinámicos que encontramos en las actividades habituales gubernamentales, científicas, humanísticas o artísticas. Esta fase buscó también crear conciencia en aspectos como la propiedad intelectual y la privacidad de datos personales a través de sus textos y discursos ante personas y organizaciones.

Recursos Documentales del Proyecto de Preservación InterPARES.

Este conjunto de lineamientos es uno entre muchos de los recursos documentales creados durante las etapas 1 y 2 con el fin de ayudar al entendimiento de la naturaleza de los documentos de archivo digitales y preparar el desarrollo de métodos para la creación confiable y exacta, y la conservación y preservación auténticas. Estas invaluables herramientas pueden y deben ser usadas por personas, organizaciones y cuerpos gubernamentales como guías para trabajar con sus cuerpos documentales. Algunos de esos recursos documentales se describen en la siguiente página, si bien el conjunto total de ellos puede ser consultado en **http://www.interpares.org**

Rc Recursos

1.Requisitos de Autenticidad. Este recurso documental de InterPARES 1 está conformado por dos conjuntos de requisitos utilizados para evaluar y conservar la autenticidad de documentos de archivos digitales; un conjunto de ellos para los creadores y otro conjunto para los preservadores de los documentos. El conjunto anterior a éstos, conocido como los ***Requisitos de Referencia***, está formado por aquellos que apoyan la presunción de autenticidad de los documentos de archivo de un creador antes de que éstos sean transferidos al resguardo de un preservador. El conjunto posterior, conocido como los **Requisitos básicos de autenticidad**, está formado por los requisitos que sostienen la producción de copias auténticas de documentos de archivo ya bajo la custodia de un preservador y conservados dentro de su sistema de preservación.

2. Plantilla para Análisis. Este recurso documental de InterPARES 1 permite desagregar un documento de archivo digital en sus cuatro partes constitutivas: forma documental, anotaciones, soporte o medio y contexto (el marco de trabajo o acción en el cual participa el documento de archivo, y son: administrativo, de procedencia, procedimental, documental y tecnológico). La plantilla define cada parte de cada elemento de forma, explica su propósito e indica si y hasta donde esa parte o elemento es un instrumento al momento evaluar la autenticidad del documento de archivo. En un nivel más básico, la plantilla sirve como una lista de verificación con definiciones que ayudan al usuario a determinar desde el principio si en efecto se trata de un documento de archivo.

3. Marco de Referencia de Políticas. Este recurso de InterPARES 2 está conformado por dos juegos de principios para la creación y preservación de documentos de archivo digitales; Ambos ayudan a estructurar la relación de los documentos de archivo entre creadores y preservadores al proveer una guía que establece un marco integral de referencia dentro del cual creadores y preservadores pueden desarrollar políticas consistentes e integradas de ambientes que lleven a una preservación efectiva y coordinada de los documentos de archivo.

4. Guía del Creador Personal. Este documento.

5. Guía del Preservador. Este recurso documental de InterPARES 2 provee recomendaciones concretas para cualquier organización responsable de la preservación a largo plazo de documentos de archivo digitales.

6. Dos Modelos de Administración de Documentos de Archivo. Este recurso documental de InterPARES 2 describe tanto en forma gráfica como textual todas las actividades importantes y acciones específicas que deben ser realizadas, así como las entradas, salidas, limitantes y controles que deben usarse para crear, administrar y preservar documentos de archivo auténticos y confiables. Ambos modelos caracterizan los datos e información que deben ser colectados, almacenados y utilizados en apoyo a la gestión documental.

Modelo de la Cadena de Preservación (Chain of Preservation ó COP Model) . Se basa en el concepto del *"ciclo de vida de documentos de archivo"* y es adaptable a situaciones específicas de creadores, administradores y preservadores.

Modelo de Gestión Documental de Archivos Orientado a Organizaciones –Business-Driven Recordkeeping Model– o simplemente BDR Model. Este modelo se basa en el concepto del *"continuum de los documentos de archivo"* y se construye sólo bajo la perspectiva del creador.

7. Base de Datos de Términos. Este recurso en línea contiene glosario, diccionario y ontologías. El **glosario** es una lista autorizada de términos y definiciones vitales para la comprensión de los documentos de archivo digitales. El **diccionario** facilita la comunicación interdisciplinaria, ya que contiene multidefiniciones en múltiples disciplinas, tales como la computación, bibliotecología y ciencias de la información, humanidades, etc. Las **ontologías** categorizan e identifican relaciones explícitas entre los conceptos de los documentos de archivo.

8. Metadatos, Registro de Descripción Archivística y Sistema de Análisis (MADRAS). Este recurso de InterPARES 2 está en-línea y consiste en un repositorio central de esquemas para ayudar a la identificación de conjuntos de metadatos o de combinaciones de elementos provenientes de grupos distintos útiles para tareas de gestión documental y preservación a largo plazo. Provee recomendaciones acerca de cómo cada esquema puede ser extendido o modificado para lograr la fiabilidad, autenticidad y necesidades de preservación de los documentos de archivo creados en el dominio, comunidad o sector específico del usuario.