Desarrollo de políticas y procedimientos para la preservación digital

Traducción al español:
Alicia Barnard, Alejandro Delgado
y Juan Voutssás

Serie: Temas
fundamentales de
preservación digital

ARCHIVO GENERAL DE LA NACIÓN

Dirección General: Mercedes de Vega
Dirección General Adjunta de Administración: Alba Alicia Mora Castellanos
Dirección de Publicaciones y Difusión: María Fernanda Treviño Campero
Departamento de Publicaciones: José María Rodríguez González

Coordinación Editorial: José María Rodríguez González
Diseño y formación: Alejandro Amaro Rosas
Diseño de portada: Alejandro Amaro Rosas
Corrección de estilo: Ma. del Carmen Gutiérrez Haces y Francisco J. González Ruiz
Asistencia editorial: Roberto del Vecchyo Calcáneo

Desarrollo de políticas y procedimientos para la preservación digital
Traducción al español: Alicia Barnard, Alejandro Delgado y Juan Voutssás

Archivo General de la Nación
Eduardo Molina núm. 113
Col. Penitenciaría
Deleg. Venustiano Carranza, C.P. 15350
Ciudad de México

Primera edición: Marzo de 2017

Contenido

Agradecimientos

Muchas personas contribuyeron a la creación de los ocho módulos que integran esta serie, en particular, los estudiantes de doctorado de la Universidad de la Columbia Británica, Elizabeth Shaffer, Corinne Rogers, Donald Force y Elaine Goh, quienes elaboraron los borradores de los contenidos basados en los trabajos de InterPARES 1 y 2, así como los casos de estudio desarrollados en InterPARES 3.

También agradecemos a los numerosos asistentes de investigación quienes elaboraron casos de estudio para todos los módulos así como al equipo de InterPARES en Canadá, a un sinnúmero de investigadores internacionales involucrados con este proyecto y, por supuesto, a su directora, Luciana Duranti.

Finalmente, nuestra gratitud a todos aquellos que revisaron y comentaron los módulos, con una mención especial a los investigadores John McDonald, consultor de administración de información (módulos 1, 2, 7 y 8), Jim Suderman, director del despacho de acceso a la información de Toronto (módulo 3), Evelyn McLellan, archivista de sistemas de Artefactual Systems, Inc. y Paul Hebbard, archivista administrador de documentos de archivo de la Universidad Simon Fraser (módulo 6).

Prefacio a la edición en inglés

Digital Records Pathways: Topics in Digital Preservation es una iniciativa educativa desarrollada en conjunto por el International Congress on Archives (ICA) y The International Research on Permanent Authentic Records in Electronic Systems (InterPARES) con el propósito de ofrecer capacitación a archivistas y profesionales que manejan documentos en cuanto a la producción, la administración y la preservación de documentos de archivo digitales auténticos, fiables y usables. El programa asume que el lector cuenta con una sólida base en cuanto a los conceptos fundamentales de la administración de archivos y en la teoría archivística, y sobre esa suposición se elaboró esta serie modular.

La serie está formada por ocho módulos más un glosario en donde se ha conjuntado terminología de acuerdo con la base de datos del ICA. Ésta aborda los conocimientos teóricos y prácticos necesarios para establecer el marco de referencia, la estructura de gobernanza y los sistemas requeridos para administrar y preservar documentos de archivo digitales, a través de su ciclo de vida. Cada módulo se refiere, específicamente, a un tema relevante para la administración o la preservación de los documentos de archivo. Todos los módulos se han diseñado de tal manera que pueden ser estudiados en forma independiente o en conjunto.

Prefacio a la edición en español

Desarrollar materiales educativos con el fin de apoyar las tareas de preservación digital en instituciones y organizaciones fue uno de los objetivos del Proyecto de Investigación Internacional para la Preservación de Documentos de Archivo Electrónicos, InterPARES 3 (2007-2012), el cual dio como resultado la serie en inglés de ocho módulos de capacitación con el título Digital Records Pathways: Topics in Digital Preservation.

No obstante que los archivos digitales –también llamados electrónicos–, se producen en la actualidad en volúmenes insospechables, el conocimiento de los archivistas y gestores de documentos en cuanto a la producción, conservación y preservación de los mismos aún es limitado, entre otros factores, a causa de la escasez de materiales de capacitación en idioma español.

Lo anterior fue el motivo para que Alicia Barnard y Juan Voutssás, miembros del Team México que formó parte del Proyecto InterPARES 3, junto con Alejandro Delgado, de España, se dieran a la tarea de traducir a nuestro idioma los ocho módulos de la citada serie, los cuales fueron publicados inicialmente en formato electrónico por el Proyecto InterPARES 3.

El Archivo General de la Nación se une a este esfuerzo para lograr una mayor difusión de temas y tópicos sobre la preservación de archivos digitales en el entorno de los archivos de nuestro país y de aquellos de habla española en Latinoamérica, y presenta una nueva versión electrónica en español de los módulos de la mencionada serie, en espera de que coadyuven a la mejor comprensión y entendimiento de la preservación de archivos digitales y el ambiente donde los mismos se producen, conservan y preservan.

Mercedes de Vega

Acerca de ICA e InterPARES

The International Council on Archives (ICA) y The International Research on Permanent Authentic Records in Electronic Systems (InterPARES) tienen el compromiso de crear materiales didácticos para la educación continua de archivistas y administradores de documentos de archivo, construir conocimiento básico, diseminar los nuevos hallazgos y dotar a los archivistas y profesionales de los documentos de archivo del conocimiento y las competencias necesarias especializadas para la administración y la preservación de documentos de archivo digitales.

El ICA (www.ica.org) está dedicado al manejo eficaz y a la preservación de documentos de archivo, así como al cuidado y uso del patrimonio archivístico mundial y su representación, por medio de profesionales en todo el planeta. Los archivos son un recurso increíble: son un subproducto documental del quehacer humano y, por tanto, testigos irremplazables de eventos pasados, puntales de la democracia, de la identidad de individuos y comunidades, así como de los derechos humanos; pero también son frágiles y vulnerables. El ICA se esfuerza por proteger los archivos y asegurar su acceso por medio de la asesoría, el establecimiento de estándares, el desarrollo profesional y el impulso del diálogo entre archivistas, líderes, productores y usuarios de archivos.

El ICA es una organización neutral, no gubernamental; sus miembros operan por medio de las actividades propias de cada membresía. Por más de sesenta años, el ICA ha unido a instituciones archivísticas y practicantes, a lo largo del mundo, para asesorar acerca de la buena administración archivística y la protección física del patrimonio registrado, para producir estándares reconocidos, buenas prácticas e impulsar el diálogo, el intercambio y la diseminación del conocimiento y experiencia más allá de fronteras internacionales. Con aproximadamente

mil quinientos miembros en 195 países y territorios, el credo del Consejo ha sido aprovechar la diversidad cultural de sus integrantes para entregar soluciones eficaces y una profesión flexible e imaginativa.

El proyecto InterPARES (www.interpares.org), pretende desarrollar conocimiento original y esencial para la conservación, a largo plazo, de documentos de archivo producidos y almacenados en formatos digitales, así como proveer una base sólida para estándares, políticas, estrategias y planes de acción capaces de asegurar la longevidad de los materiales documentales y la capacidad de sus usuarios para confiar en su autenticidad. InterPARES se ha desarrollado en tres etapas:

- InterPARES 1 (1999-2001). Esta etapa se enfocó en el desarrollo de la teoría y los métodos que pudiesen asegurar la preservación de la autenticidad de los documentos de archivo producidos y conservados en bases de datos y sistemas de gestión de documentos de archivo, durante el curso de las actividades propias de su administración. Los hallazgos de esta etapa presentaron el punto de vista del preservador de los documentos de archivo.
- InterPARES 2 (2002-2007). Se continuó investigando acerca de temas relativos a la autenticidad, fiabilidad y exactitud durante todo el ciclo de vida de los documentos de archivo, desde su producción hasta su conservación permanente. Se enfocó en aquellos documentos de archivo producidos en entornos digitales dinámicos e interactivos a lo largo de actividades artísticas, científicas y gubernamentales.
- InterPARES 3 (2007-2012). Se construyó sobre la base de los hallazgos de las primeras dos etapas en conjunto con otros proyectos de preservación digital de distintas partes del mundo. Se llevó

la teoría a la práctica al trabajar con archivos y unidades archivísticas dentro de organizaciones que tuvieran recursos humanos y financieros limitados, con el fin de implementar en ellas programas sólidos de gestión y preservación de archivos.

Público objetivo

El público objetivo para el cual está destinado este programa se compone de archivistas, gestores documentales y profesionales de la gestión archivística, interesados en ampliar sus capacidades en la administración de documentos de archivo digitales. En conjunto, los módulos conforman todo un paquete de recursos documentales para la educación continua de profesionales, con especial énfasis en aquellos temas que impactan en la preservación de documentos de archivo, auténticos, fiables y exactos.

Cómo usar la serie

Cada módulo de la serie está formado por conocimiento teórico y metodológico, así como por aplicaciones prácticas ilustradas en casos de estudio y escenarios modelo. Si bien los módulos fueron desarrollados por el equipo canadiense de InterPARES y, por tanto, ejemplificados en un contexto propio a aquél, son adaptables a un dominio específico o ámbito jurídico. Para una mayor aplicabilidad se han traducido a los idiomas de los miembros del ICA.

Los módulos pueden estudiarse por separado o en conjunto, de acuerdo con cada necesidad o interés, pues abarcan un rango amplio de competencias requeridas; pueden ser estudiados individualmente u ofrecerse a grupos como asociaciones profesionales o instituciones de capacitación laboral. Algunos de los módulos incluyen formularios

que pueden adaptarse a universidades o asociaciones profesionales para el desarrollo de cursos curriculares, o como materiales de capacitación para estudiantes y profesionales de la gestión o preservación documental digital. Las universidades y asociaciones profesionales son libres de adaptar los materiales para desarrollar sus propios cursos curriculares o de capacitación. Se sugieren recursos adicionales en la web que se identifican a lo largo de los módulos con el icono:

o bien, cuando se trata de información complementaria ubicada en anexos o en los mismos módulos de la serie, se distinguen con la figura:

Objetivos

Los módulos tienen los siguientes objetivos:

- Aportar recursos educativos basados en investigación actual sobre temas de administración de archivos digitales para beneficio de miembros de asociaciones profesionales relacionadas con esa temática.
- Proporcionar a los profesionales de archivos, con conocimiento teórico y procedimental, habilidades estratégicas necesarias para desarrollar, implementar y supervisar un sistema de gestión o de preservación documental.
- Ilustrar conceptos teóricos con aplicaciones prácticas mediante ejemplos reales extraídos de casos de estudio, asociados con contextos administrativos y tecnológicos específicos.

- Proporcionar contenidos y estructura a programas educativos universitarios para implementar cursos sobre administración o preservación de archivos.

Arquitectura modular del programa

Los primeros dos módulos presentan los fundamentos de todo programa de preservación de documentos de archivo digitales; proporcionan los conocimientos propedéuticos sobre los demás módulos. Los siguientes tres módulos tratan temas generales contemporáneos que competen a la preservación digital: el papel de la cultura organizacional, una visión general de los metadatos y de la valoración en el contexto de la administración de documentos de archivo fuera del sistema de gestión documental Electronic Recordkeeping Management System (ERMS). En los tres últimos módulos se abordan temas específicos de interés contemporáneo: la administración de correos electrónicos, la preservación de documentos de archivo en ambientes web, y los temas emergentes acerca del creciente auge del cómputo en la nube (Tabla 1).

Tabla 1 Arquitectura modular del programa

Tema del módulo	Aspecto
1. Marco de referencia para la preservación digital. 2. Desarrollo de políticas y procedimientos para la preservación digital.	Fundamentos
3. Cultura organizacional administración de archivos. 4. Breviario de metadatos. 5. Control de los documentos de archivo digitales.	Generalidades
6. Correo electrónico. 7. Documentos de archivo en ambientes web. 8. Cómputo en la nube.	Específico
Base de datos internacional, terminología.	Fundamentos

Cada módulo contiene todos o algunos de los siguientes elementos:

- Panorama del tema y alcance del módulo.
- Objetivos y aprendizajes esperados del módulo.
- Metodología o procedimientos para la aplicación y desarrollo del módulo.
- Formularios (cuando apliquen) para facilitar la implementación del módulo.
- Ejemplos, casos de estudio o escenarios (cuando apliquen) con situaciones reales acerca del tema.*
- Ejercicios de los puntos clave del aprendizaje.
- Preguntas de revisión que optimicen la comprensión y entendimiento del tema.
- Recursos adicionales.
- Lecturas, estándares y otros recursos de referencia.

Cuando se ha considerado apropiado, se hace la distinción de la administración y preservación de documentos de archivo activos en contraste con las responsabilidades relativas a éstos que ya no son requeridos para actividades cotidianas de la organización y que serán preservados por su productor o por un tercero de confianza.

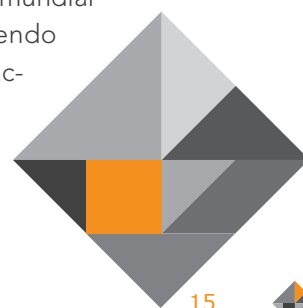
* Los ejemplos y casos de estudio citados en los módulos provienen de casos reales de InterPARES 3 y tienen como propósito apoyar la experiencia de aprendizaje del módulo. Si bien reflejan los hallazgos de investigación del proyecto, no necesariamente deben ser tomados como plantillas para ser aplicadas a pie juntillas en todos los casos. Cada organización (productor o preservador) es diferente y la preservación de sus documentos de archivo debe tomar las mejores prácticas desde una perspectiva práctica en cuanto a la viabilidad de una cierta implementación.

Alcance

La serie comprende los siguientes ocho módulos:

Módulo 1 Un marco de referencia para la preservación digital.
Módulo 2 Desarrollo de políticas y procedimientos para la preservación digital.
Módulo 3 Cultura organizacional y sus efectos en la administración de archivos.
Módulo 4 Breviario de metadatos.
Módulo 5 Estrategias para lograr el control de los documentos de archivo digitales en ambientes de red distribuidos.
Módulo 6 Gestión y preservación de correo electrónico.
Módulo 7 Gestión y preservación de documentos de archivo en ambientes web.
Módulo 8 Introducción al cómputo en la nube.

Para asegurar un entendimiento generalizado y reducir un potencial riesgo de confusión que pudiese surgir de prácticas regionales o jurisdiccionales, estos módulos están apoyados por una base de datos de administración de archivos la cual refleja los usos habituales y prácticos en 16 idiomas. Esta base, desarrollada conjuntamente por el ICA e InterPARES está disponible en www.web-denizen.com/. Dicho recurso dinámico continuará creciendo y desarrollándose en la medida en que los miembros de la comunidad archivística mundial puedan participar agregando o enriqueciendo las definiciones usadas en su región de práctica. Pueden verse ciertos términos específicos, en breves glosarios existentes en cada módulo, aún no incluidos en la base de datos.



Introducción

Todos los individuos y organizaciones crean documentos de archivo en el curso de sus asuntos cotidianos. Los documentos de archivo documentan transacciones y proporcionan la base para la futura toma de decisiones. Confiamos en los que creamos para brindar pruebas de nuestras decisiones y transacciones, derechos y responsabilidades. Además de ser instrumentos de responsabilidad, los documentos de archivo bien gestionados, auténticos y fiables pueden servir, también, como fuentes de información importantes y de confianza para la memoria y la futura toma de decisiones. Sin embargo, puede ser que los documentos de archivo que no están bien gestionados no soporten el escrutinio cuando son requeridos como evidencia de transacciones o a efectos de responsabilidad. Para satisfacer estos fines, los documentos de archivo deben crearse, mantenerse y preservarse para ser confiables, esto es, que sean fiables, exactos y auténticos; y deben seguir siendo accesibles y utilizables a lo largo del tiempo y de los cambios tecnológicos.

Una política de preservación digital proporciona el marco para la acción y la planificación que asegure el mantenimiento y la preservación a largo plazo de los documentos de archivo de una organización. Seguir una política de preservación digital a lo largo de la vida activa de los documentos de archivo facilitará la preservación a largo plazo de los documentos de archivo inactivos; ya sea que el creador preserve los documentos de archivo o lo haga una tercera parte fiable.

Alcance

Dependiendo del marco de políticas dentro de una organización, puede ser que los requisitos de política que pertenecen a la preservación se incorporen a una política existente de administración

de archivos, a las políticas que regulan los programas y/o sistemas de la organización, o que se reflejen en una política autónoma de preservación digital. Este módulo esboza el desarrollo de una política de alto nivel y puede ser utilizado tanto por la organización que crea el documento de archivo como, en otros casos, por el conservador del documento de archivo.

Fines y objetivos

El objetivo de este módulo es explicar el propósito y los beneficios de una política de preservación digital y proporcionar el conocimiento y las herramientas necesarios para crearla. Este módulo le guía en el desarrollo, la redacción y la implantación de una política de preservación digital eficaz dentro de su organización e incluye una metodología para la creación de políticas, en general, herramientas prácticas para ayudar en su desarrollo, ejemplos de políticas de preservación digital existentes y enlaces a recursos complementarios para ayudarle en el desenvolvimiento de dichas políticas y procedimientos.

Resultados de la formación

Al finalizar este módulo será capaz de:

- Comprender el propósito y los beneficios de una política de preservación digital y de los procedimientos que la acompañan.
- Distinguir entre política y procedimientos.
- Comprender los fundamentos del desarrollo de una política de preservación digital, identificar qué necesidades están excluidas en (y excluidas de) una política de preservación digital.
- Comprender las cuestiones que tienen que considerarse cuando se implanta una política de preservación digital.

- Disponer de las herramientas fundamentales para llevar a cabo el desarrollo de una política de preservación digital dentro de su organización.
- identificar dónde localizar información y recursos adicionales que ayuden en el desarrollo y la implantación de la política.

¿Qué es una política?

Una política es una serie de reglas y principios que guían la toma de decisiones y las acciones para lograr los resultados deseados para un asunto o fin en particular. La política debería aprobarse a un alto nivel dentro de una organización y:

- Ser no prescriptiva.
- Tecnológicamente neutral.
- Soportar la estructura de gobierno y la cultura organizativa de una organización.

La política proporciona un marco que dicta el alcance y los requisitos de los procedimientos. Se sitúa dentro del contexto más general de la organización y ayuda a desarrollar el mandato de la organización. La política no delinea acciones en particular; este es el papel de los procedimientos.

¿Qué son los procedimientos?

Los procedimientos son acciones u operaciones prescriptivas que, al ejecutarse, dan como resultado un producto de salida prescrito. Son las acciones que se establecen para permitir que la teoría se ponga en práctica. Deberían instaurarse y esbozarse procedimientos dentro de una organización, ya que éstos reflejan los fines y requisitos establecidos en la política. Puesto que son específicos del contexto, cambian de manera más frecuente que la política, de modo que es más fácil

modificarlos a medida que se requiera. Las organizaciones incorporan a menudo elementos de los procedimientos en la política; este módulo recomienda que la política se mantenga a un alto nivel. Posteriormente, los procedimientos pueden desarrollarse dentro de una organización para dar soporte a la política y reflejar las necesidades y requisitos específicos de la organización.

¿Qué es la preservación digital?

Las organizaciones están creando un número cada vez mayor de documentos digitales de archivo. A diferencia de los documentos de archivo tradicionales (por ejemplo, sobre papel o película), los documentos digitales de archivo son vulnerables a pérdida o corrupción. A causa de la velocidad de los cambios tecnológicos, las organizaciones deben considerar las cuestiones de preservación de sus documentos digitales de archivo, incluso mientras aún están en uso activo. Para asegurar la autenticidad, la fiabilidad y la accesibilidad de los documentos de archivo a lo largo del tiempo, las organizaciones tienen que tomar en consideración cuestiones de preservación en el momento de la creación. Esto significa abordar la cuestión de la preservación en la etapa de planificación del diseño del programa o sistema, incluso antes de que los documentos de archivo se hayan creado.

> La preservación digital es el proceso de mantener materiales digitales entre diferentes generaciones de tecnología a lo largo del tiempo, con independencia del lugar en que residen (InterPARES).

El propósito de una política de preservación digital

Varios proyectos de investigación internacionales están buscando, actualmente, soluciones y construyendo herramientas

tecnológicas para la preservación digital. Sin embargo, la tecnología es sólo parte de la solución. Para ser eficaz, la preservación digital debería soportar los fines y objetivos de una organización mediante marcos y políticas institucionales.

Requisitos fundamentales

Una política de preservación digital debería asegurar que:

- Los documentos digitales de archivo se generan y mantienen auténticos y fiables.
- Los documentos digitales de archivo siguen siendo utilizables a lo largo del tiempo.
- Las prácticas de gestión de documentos se adhieren a normas y buenas prácticas pertinentes.
- Los documentos digitales de archivo se mantienen y preservan de acuerdo con todos los requisitos reguladores pertinentes.
- Los documentos de archivo identificados para su conservación a largo plazo son susceptibles de ser conservados.

Una política de preservación digital facilita la gestión eficaz de documentos digitales de archivo, asegurando que la organización es capaz de llevar a cabo las funciones que se le han encomendado. La gestión eficaz continuada y el acceso a los documentos digitales de archivo asegura que éstos están disponibles dentro de una organización, para dar soporte a las operaciones y a la toma de decisiones.

La investigación en documentos digitales de archivo ha mostrado que no es posible preservarlos, sino sólo mantener la capacidad para reproducirlos. La autenticidad, la fiabilidad y la exactitud de los documentos de archivo dependen de un marco de requisitos específicos; y la capacidad para mantener la autenticidad de los documentos de archivo a lo largo del tiempo debe considerarse cuando éstos se están produciendo.

InterPARES 2 desarrolló un marco de principios que guían la creación de políticas, estrategias y normas, que es lo suficientemente flexible como para ser implantado en diferentes entornos nacionales y para equilibrar perspectivas culturales, sociales y jurídicas, sin dejar de ser lo bastante robusto para servir como un sólido fundamento para cualquier documento de política resultante.

Véase Apéndice A en el Módulo 1: Un marco de referencia de principios para el desarrollo de políticas, estrategias y estándares para la preservación, a largo plazo, de documentos de archivo digitales.

Estos principios de InterPARES deberían situarse dentro del contexto de un objetivo de política global que establezca el vínculo entre los documentos de archivo y los asuntos de la organización.[1] Se aplican al desarrollo de políticas si el enfoque primario es la creación o la preservación de documentos de archivo:

- Los documentos digitales de archivo deben tener forma fija y contenido estable.
- Los componentes digitales de los documentos de archivo deberían crearse de tal modo que pudieran mantenerse separadamente y recomponerse a lo largo del tiempo.

[1] ISO 15489 (Management Statement: 2007) expone los siguientes objetivos que vinculan los documentos de archivo con los asuntos de la organización: 1) estrategias, que incluyen la ejecución eficaz de asuntos mediante una toma de decisiones informada; gestión del funcionamiento; mejora de la productividad; coherencia, continuidad y aseguramiento de la calidad en la gestión y en las operaciones; 2) operaciones, incluidos la provisión sensible y exacta de servicios, la gestión de recursos y el control de costes; 3) cumplimiento regulador, y protección y soporte legal; 4) responsabilidad, gobernanza corporativa, auditorías financieras y de práctica; 5) gestión del riesgo, incluidas seguridad, gestión de la reputación, planificación e implantación de la continuidad de negocios; 6) valores corporativos, incluidos franqueza, seguridad, calidad, integridad, respeto y satisfacción de las expectativas de interesados externos; 7) memoria corporativa, incluidos la innovación mediante la captura y la reutilización de conocimiento organizativo; y el uso de conocimiento estratégico para dar soporte a los asuntos.

- Los documentos de archivo deberían crearse y mantenerse de acuerdo con los propósitos que deben satisfacer; y deberían conservarse de acuerdo con el propósito y el resultado deseado de la preservación, más que en términos de las tecnologías disponibles.
- Las políticas de documentos de archivo deberían abordar expresa y separadamente las cuestiones de la fiabilidad, la exactitud y la autenticidad de los documentos de archivo.
- Debería utilizarse un sistema fiable de producción de documentos de archivo (actividades y procedimientos; y tecnologías documentales integrados), para generar documentos de archivo que puedan presumirse fiables.
- Debería utilizarse un sistema fiable de gestión de documentos para mantener documentos de archivo que puedan presumirse exactos y auténticos.
- Las decisiones de valoración y preservación deberían anidarse en todas las actividades de creación y gestión de documentos de archivo.
- Debería designarse un custodio fiable como preservador de los documentos de archivo de un creador.
- Todos los procesos de negocio que puedan contribuir a la creación o uso de los documentos de archivo deberían quedar bien documentados.
- Los derechos de propiedad intelectual de terceros unidos a los documentos de archivo deberían quedar explícitamente identificados y gestionados en los sistemas de creación y de gestión de documentos de archivo.
- Los derechos y las obligaciones con respecto a la privacidad, unidos a los documentos de archivo, deberían quedar explícitamente identificados y administrados en los sistemas de creación y gestión de documentos de archivo.

- Deberían establecerse procedimientos para compartir documentos de archivo entre jurisdicciones, sobre la base de los requisitos legales vigentes.
- Las reproducciones realizadas en el curso usual y ordinario de negocios, o a efectos de preservación, tienen el mismo efecto que la primera manifestación del documento de archivo y son consideradas copias auténticas.

Estos principios están contenidos en la metodología y la plantilla que siguen.

Desarrollo de políticas

El desarrollo de políticas para la administración y la preservación a largo plazo de documentos digitales de archivo en una organización está guiado por una metodología de investigación de la acción, la cual se basa en una aplicación reiterada de prácticas que incluyen la recolección de datos, el diálogo cooperativo y la toma de decisiones participativa.

Aunque este módulo se enfoca sobre el desarrollo de una política de preservación digital, la metodología que sigue puede aplicarse con éxito al desarrollo de un plan estratégico más general; o adaptarse a cualquier desarrollo de políticas o procedimientos. El flujo de trabajo de la recolección y el análisis de datos proporciona valiosos datos acerca de la organización (agencia u oficina); y de los documentos de archivo que crea, mantiene o preserva. En el contexto de la discusión que sigue, el flujo de trabajo se presenta primariamente como una herramienta de desarrollo de políticas, distinguiendo entre políticas y procedimientos cuando es adecuado o necesario.

El proceso de desarrollo de políticas es establecido para cada organización a nivel de la gestión superior u otro cuerpo administrativo o regulador. Tiene que encontrarse vigente un proceso mediante el cual pueda desarrollarse y aprobarse. Sin éste en vigor, es probable que fracasen incluso los mejores esfuerzos por desarrollar e implantar políticas. La identificación de la necesidad de una política de administración de archivos en general –y de procedimientos que regulan los documentos digitales de archivo, en particular–, puede proceder del administrador de archivos o de la oficina de administración de archivos; del administrador de negocio o de la administración superior. La creación de una política exitosa es resultado del esfuerzo de un equipo cooperativo. Los administradores de archivos obtendrán

su mayor éxito si sus administradores de negocio representan la necesidad de una política a la administración *senior*.

Una vez que la persona o la oficina que trata de iniciar el desarrollo de una política ha recibido la aprobación necesaria del cuerpo *senior*, el siguiente flujo de trabajo conducirá al desarrollo de una política que asegure que:

- Los documentos digitales de archivo se crean fiables y exactos; y se mantienen auténticos.
- Los documentos digitales de archivo siguen siendo utilizables a lo largo del tiempo.
- Las prácticas de gestión de documentos se adhieren a normas y buenos procedimientos relevantes.
- Los documentos de archivo se mantienen y preservan de acuerdo con cualquier requisito regulador relevante.
- Los documentos de archivo identificados para su preservación a largo plazo son susceptibles de ser preservados.

De manera más específica, los documentos digitales de archivo regulados por tal política serán susceptibles de satisfacer sus funciones de negocio con independencia de la tecnología utilizada para crearlos, mantenerlos y almacenarlos. Tendrán contenido estable y forma fija; se puede presumir de ellos que son fiables, auténticos y exactos a lo largo de todo su ciclo de vida; los derechos de privacidad y de propiedad intelectual serán explícitamente identificados y gestionados; y su uso y acceso continuado quedarán asegurados.

Ejercicio:

- Identifique el nivel en el que el desarrollo y la aprobación de la política tiene lugar en su organización.
- ¿Qué políticas existentes cubren la administración de archivos? Si su organización tiene una política de administración de archivos, ¿cubre explícitamente la preservación digital?

El siguiente diagrama de flujo de tareas delinea el proceso de desarrollo de una política de preservación digital.

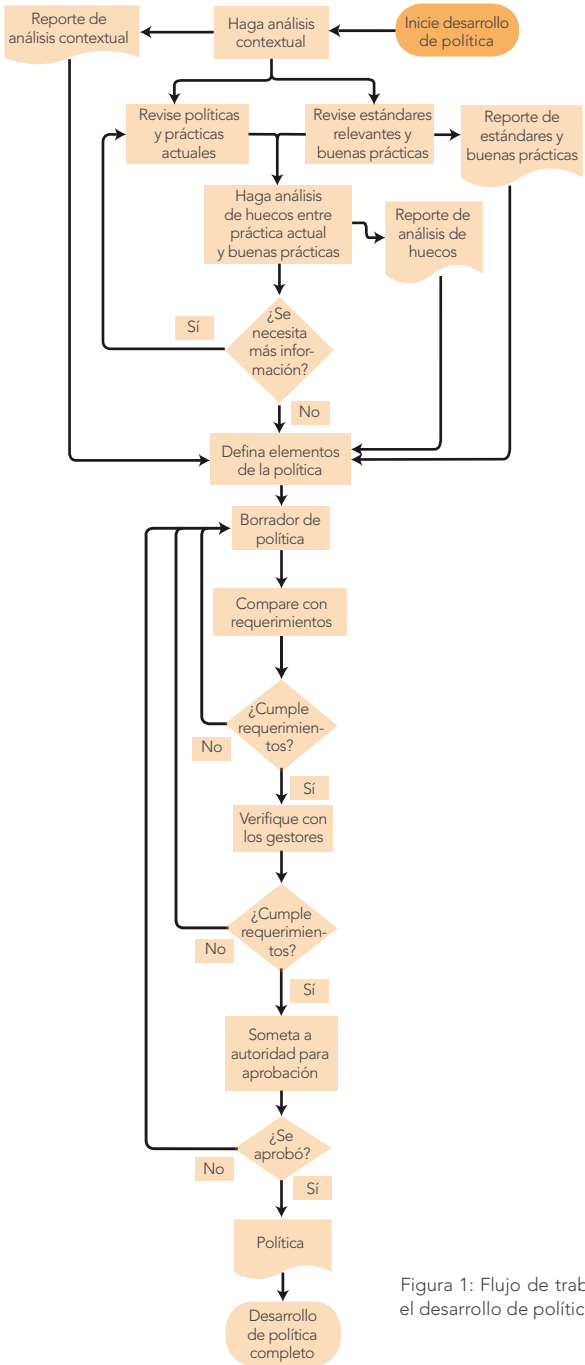


Figura 1: Flujo de trabajo para el desarrollo de políticas.

Narrativa del diagrama de flujo de trabajo

El proceso de crear una política comienza identificando la necesidad de regular la ejecución y la práctica mediante instrumentos formales. La persona o el departamento responsable construirán un caso para que articule esa necesidad y posicione la política propuesta en su contexto organizacional. Después, el caso debe ser presentado a las autoridades adecuadas. Resulta crítico, cuando se desarrolla una política, asegurar el compromiso de todas las partes interesadas. Si las personas que desarrollan, aplican o supervisan la política no están comprometidas en su implantación, la política no logrará los resultados pretendidos y será una fuente continua de frustración.

Los factores desencadenantes que conducen al reconocimiento y a la expresión de la necesidad de una política deberían proceder de una cuestión reconocida de negocio. Puede que esto implique múltiples o una única función de negocio, quizá central. Sin embargo la necesidad, si se expresa de manera general, debería reflejar siempre una perspectiva de negocio (por ejemplo, los sistemas que dan soporte al principal propósito de negocio de una organización están generando documentos digitales de archivo que tienen que retenerse por motivos legales y organizacionales durante periodos extensos de tiempo, y la organización desea desarrollar una política para guiar el proceso de retención y preservación).

Una vez que se recibe la aprobación para desarrollar la política, los redactores comienzan ejecutando una investigación, identificando los resultados requeridos de la política, entrevistando a las partes interesadas, escribiendo borradores, presentándolos para revisión y examinando la política hasta que esté lista para su aprobación e implantación final.

Iniciar el desarrollo de la política. El primer paso es ejecutar una investigación que permitirá a los redactores establecer

claramente los fines y los resultados de la política; anidarla en una red de políticas existentes según sea necesario; y que resulte contextualmente relevante en la organización. La investigación consiste en ejecutar un análisis contextual, revisar e investigar la práctica actual y las buenas prácticas de la industria; y ejecutar un análisis de huecos para identificar lo que debe incluirse en la política.

Elaborar un análisis contextual. Esto permite reunir información acerca de la organización o el departamento que influirá en la política o en los procedimientos que se estén desarrollando: su estructura administrativa; sus obligaciones legales y reguladoras con respecto a sus documentos de archivo; pautas y normas que influyen en la creación de documentos de archivo; mantenimiento y uso; sus requisitos y restricciones para la creación y la gestión de documentos de archivo, incluida la cultura de negocio de la organización, las restricciones de personal y las restricciones tecnológicas.

Véase Apéndice A: Análisis contextual.

Se reunirá información mediante entrevistas y análisis de la información impresa de su organización. Entrevistará a administradores y a quienes toman decisiones; a administradores de archivos y a otros responsables de la administración de archivos. Leerá informes anuales, planes de trabajo y estratégicos; documentación legal y legislación; y cualquier otro material que le ayude a comprender mejor el marco dentro del cual funcionarán la política y los procedimientos en desarrollo.

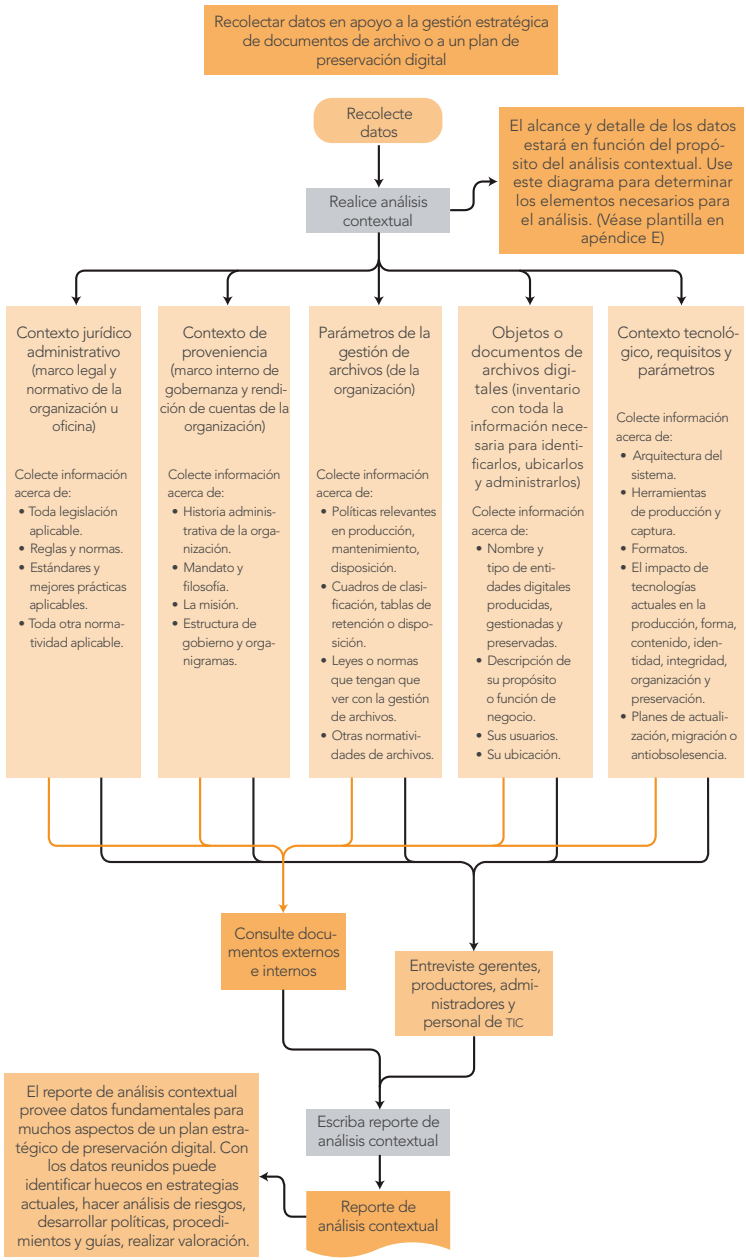


Figura 2: Ejecutar un análisis contextual.

Ejercicio:

- ¿Quiénes son los decisores clave que entrevistará primero y cuál es su impacto dentro de la organización sobre los requisitos de administración de archivos? Considere a los gestores de TIC y de los departamentos legales.
- ¿Cuál es la relación entre el personal de TIC y el de administración de archivos en su organización?

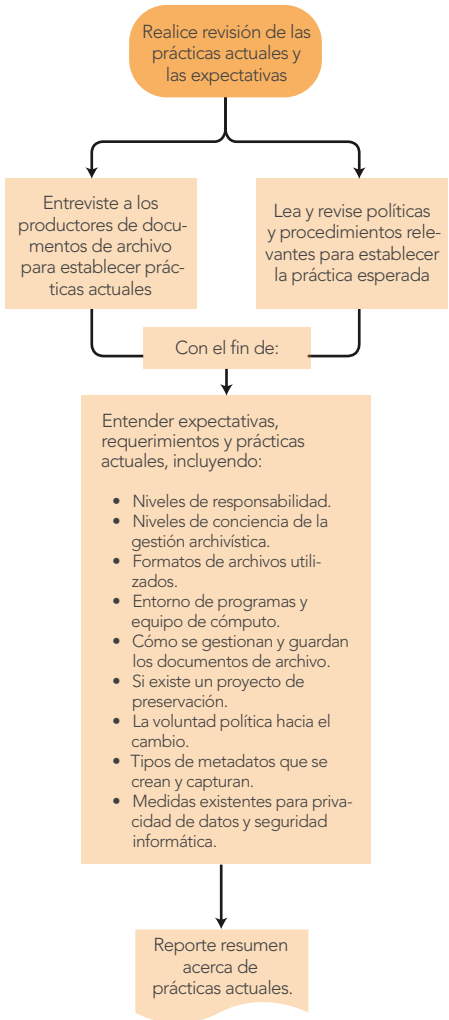


Figura 3: Revisar las prácticas actuales.

Realizar una revisión de las prácticas actuales. Lo cual le dará una visión comprensiva acerca del modo en que los documentos de archivo se crean y gestionan actualmente en su organización. Entrevistará a los creadores de documentos de archivo y analizará las políticas ya existentes que regulan y obligan a la administración de archivos.

Véase el Apéndice B para ver un esbozo de la información que debería tener.

Ejecutar la revisión de normas y de buenas prácticas relevantes

Examine todas las normas y buenas prácticas que sean relevantes a su contexto organizacional. Identifique los puntos clave que son relevantes para su organización y por los cuales desea considerarlas en la política o los procedimientos en desarrollo. La política de preservación digital debería dar cuenta de las estrategias clave de gestión que protegen la autenticidad, la fiabilidad, la usabilidad y la accesibilidad de los documentos de archivo, durante tanto tiempo como se necesiten, ya sea explícita o implícitamente (véase el punto 5 más abajo).

Ejercicio:

- ¿Qué políticas se tienen para la administración de archivos en su organización? ¿Alguna de las políticas existentes cubren explícitamente la preservación digital?

Realizar un análisis de huecos. Comparar las prácticas ya existentes con normas y con buenas prácticas. Establezca una concordancia entre las prácticas ya existentes y las buenas prácticas delineadas en las Recomendaciones para el creador y el preservador

de InterPARES 2; así como las normas relevantes bajo las que opera su organización. Esto le ayudará a identificar huecos que pueden subsanarse mediante el desarrollo de una política y de procedimientos. Si después de ejecutar este paso necesita más información o aclaración, regrese a los pasos anteriores.

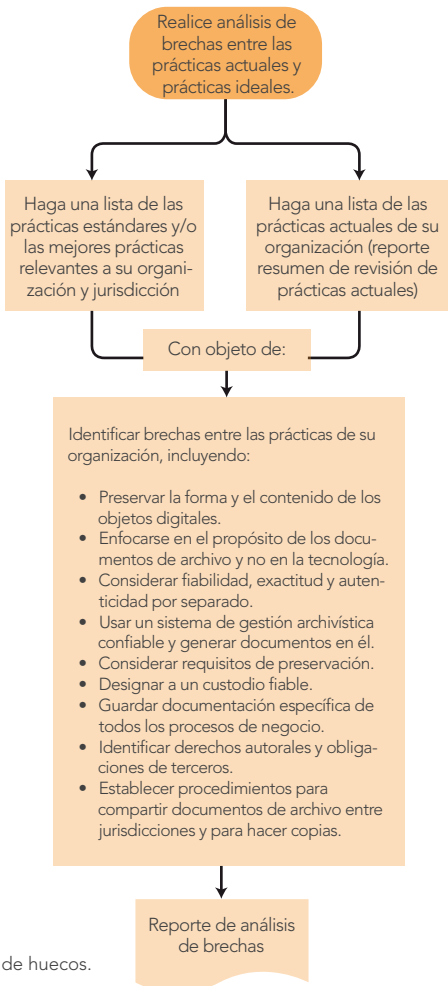


Figura 4: Análisis de huecos.

Véanse Apéndices C y D para las versiones completas de las recomendaciones para el creador y el preservador de InterPARES 2.

Su comparación debería considerar las siguientes áreas (*cabe mencionar que el nivel de granularidad es aplicable a los procedimientos más que a la política. Sin embargo, estos elementos deben ser considerados cuando se elaboran declaraciones generales de política*).

Accesibilidad

- Seleccione software y hardware interoperables.
- Seleccione software y hardware retrospectivamente compatibles.
- Adopte normas de software oficiales o de facto.
- Documente completamente todas las decisiones y cualquier personalización.
- Seleccione formatos ampliamente utilizados, no propietarios, independientes de la plataforma, no comprimidos, con especificaciones libremente disponibles, siempre que sea posible.
- Seleccione compresión sin pérdida, siempre que se requiera compresión.

Fijeza

- Verifique que los documentos digitales de archivo tengan forma fija y contenido estable.
- Dote a los documentos de archivo de variabilidad limitada (reglas fijas establecidas para la selección de contenido y forma documental que permitan variaciones conocidas, estables).

- Establezca los elementos de la presentación o la forma documental que son esenciales al significado de los documentos de archivo.

Identidad

- Asegure la integridad de los metadatos de identidad:
  - Nombres de personas (autor, redactor, generador, destinatario, receptor).
  - Título/asunto (acción o materia).
  - Forma documental (carta, informe y otros).
  - Presentación digital (formato, contenedor, codificación y demás).
  - Fechas de creación y transmisión.
  - Expresión del contexto documental (por ejemplo, código de clasificación, carpeta o directorio; y demás).
  - Indicación de adjuntos (si es aplicable).
  - Indicación del copyright u otros derechos intelectuales (si es aplicable).
  - Indicación de la presencia o la retirada de firmas digitales.
  - Indicación de otras formas de autenticación (por ejemplo, corroboración, testimonio y demás).
  - Número de versión o borrador (si es aplicable).
  - Existencia y localización de materiales duplicados fuera del sistema (indique cuál es la copia autorizada).

Integridad

- Asegúrese de que los materiales digitales contienen información que le ayudará a verificar su integridad.
- Metadatos de integridad:
  - Nombre de las personas/oficinas que los tratan.

- Nombre de la oficina/persona con responsabilidad primaria sobre la gestión (puede ser la misma que la del tratamiento).
- Indicación de anotaciones.
- Indicación de cambios técnicos a los materiales o a la aplicación.
- Restricciones de acceso (si es aplicable).
- Privilegios de acceso (si es aplicable).
- Documentos de archivo vitales (si es aplicable).
- Disposición planeada.

Organización

- Organice los materiales digitales en agrupamientos lógicos (cuadro de clasificación, metadatos de identidad).

Autenticación

- Use técnicas de autenticación que promuevan el mantenimiento y la preservación de materiales digitales.
- Independiente de la tecnología versus dependiente de la tecnología.

Protección

- Proteja los materiales digitales de acciones no autorizadas.

Copia de seguridad

- Cuide de pérdida y corrupción accidentales a los materiales digitales.

- Desarrolle una política o una rutina rigurosas que aseguren que se hace copia de seguridad diaria de su sistema.
- Seleccione e instale la mejor tecnología de copia de seguridad para su situación.

Obsolescencia

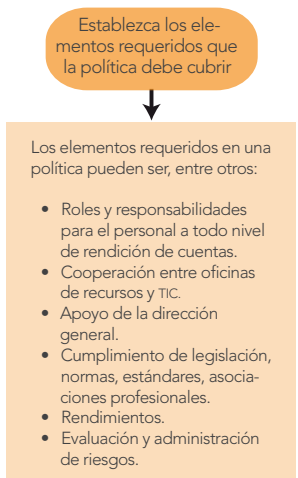
- Adopte medidas contra la obsolescencia del hardware y del software.

Conciencia

- Considere los problemas en torno a la preservación a largo plazo.

Ejercicio:

- Utilice la plantilla proporcionada en el Apéndice E para comenzar a establecer las concordancias entre los elementos requeridos para la preservación digital y sus políticas ya existentes.
- Utilice la plantilla proporcionada en el Apéndice E para comenzar a identificar los elementos requeridos que deben ser abordados en la nueva política.



Establecer los elementos requeridos que la política debe cubrir. Decida el modo en que su política asegurará que van a ser incluidos los elementos necesarios para hacer posible la creación, el mantenimiento y la preservación de documentos de archivo auténticos, fiables, exactos y accesibles. Delinee los roles y responsabilidades del personal a todos los niveles de responsabilidad, en relación con todos los documentos de archivo. Detalle las cuestiones de formación, ponderación del riesgo y conformidad.

Elementos requeridos de la política

Redactar la política para su revisión. Utilice la plantilla de política como guía.

Medir el borrador de políticas contra los requisitos. Confronte las declaraciones de política que ha transcrito contra los requisitos que ha identificado. Si su política no satisface todos los requisitos, regrese a los pasos anteriores, según sea necesario; y haga los cambios que se requieran.

Revisar con las partes interesadas relevantes. Consiga retroalimentación de las partes interesadas, para asegurarse de que el borrador de política puede implantarse tal y como se pretendía. En su caso, incorpore la retroalimentación o reúna más datos.

Presentar para su aprobación a la autoridad adecuada.

Plantilla de política

Principios

Una política de preservación de documentos digitales de archivo establece los principios generales que guían la implantación de un programa de administración y preservación de documentos digitales de archivo, asegurando la fiabilidad, autenticidad y

accesibilidad de los mismos en el espacio y a lo largo del tiempo. Una política de preservación digital proporciona orientación acerca de la administración de documentos digitales de archivo que tienen que retenerse durante periodos que podrían exceder el lapso de vida de la tecnología que originalmente los creó. Prescribe las responsabilidades y las funciones de todos aquellos en la organización que crean y utilizan documentos digitales de archivo. Debe utilizar un lenguaje que sea claro y conciso. En caso de que se utilice terminología de administración de archivos y archivística, los usuarios de la política serán dirigidos a un glosario. Debe supervisarse y auditarse para asegurar su eficacia y revisarse de manera regular.

Elementos de la política

La política debe abordar:

- Propósitos/objetivos.
- Alcance.
- Mandato.
- Declaración de política.
- Roles y responsabilidades.
- Definiciones.
- Fuentes relacionadas.
- Control de versiones.
- Revisión de la política.

Propósito y objetivos

Debe comenzar con una sección introductoria que alinee los fines y los objetivos de la política, con los fines y los objetivos de la organización. Las políticas que regulan la creación, el mantenimiento y la preservación de documentos digitales de archivo deberían abordar las cuestiones de fiabilidad, exactitud y autenticidad del documento de archivo.

Los ejemplos que siguen están tomados de los casos de estudio de InterPARES 3. Muchas de las pequeñas y medianas organizaciones que participaron como socios de pruebas en InterPARES 3 trataban de desarrollar políticas y procedimientos que les ayudaran a administrar sus documentos digitales de archivo. Los ejemplos se ofrecen para ayudar a comenzar el proceso de iniciativas de desarrollo de políticas y para dar soporte a la experiencia de aprendizaje de este módulo. Aunque reflejan los principios y las recomendaciones desarrollados a lo largo de la investigación de InterPARES, no están orientados necesariamente a ser considerados plantillas de buenas prácticas. Cada organización es diferente y debe enfocarse con una visión práctica de la implantación de los principios.

Ejemplos:

Ejemplo 1. cIRcle: University of British Columbia's Digital Repository (cIRcle), Política de Preservación Digital.

El propósito de la Política de Preservación Digital cIRcle es garantizar que se emprendan acciones para asegurar la preservación a largo plazo del contenido digital de cIRcle. Esta política actúa como una guía autorizada para la preservación a largo plazo de los contenidos de cIRcle y proporciona un marco para guiar las prácticas de preservación.

Ejemplo 2. British Columbia Institute of Technology (BCIT), Política de Preservación Digital.

Esta política actúa como una guía autorizada sobre la preservación a largo plazo de documentos digitales de archivo en el BCIT y proporciona una visión general comprehensiva de la función de preservación digital a largo plazo.

Los objetivos de esta política son:

- Dar soporte a la identificación de las características significativas de los documentos digitales de archivo que tienen que protegerse para mantener su exactitud, fiabilidad y autenticidad;

- Asegurar que los creadores y custodios de documentos digitales de archivo del BCIT están informados de sus papeles y responsabilidades en la creación, el mantenimiento y la disposición de los documentos digitales de archivo identificados para su preservación permanente y a largo plazo y;
- Dar soporte a la accesibilidad permanente y la preservación continua de documentos digitales de archivo que serán considerados fidedignos para efectos legales, administrativos e históricos en el largo plazo.

Alcance

El alcance de la política debería indicar los objetos digitales que están cubiertos por la política y los individuos o departamento(s) a quienes se aplica la política.

Ejemplos

Ejemplo 1. cIRcle, Política de Preservación Digital.

Esta política cubre todos los objetos digitales enviados a cIRcle.

Ejemplo 2. BCIT, Política de Preservación Digital.

¿A quién se aplica esta política?

A todos los empleados del BCIT (incluidos académicos, personal y administradores); y a todas las escuelas y departamentos que generan documentos digitales de archivo.

Alcance de la política de preservación de documentos digitales de archivo:

- La política del BCIT para la preservación de documentos digitales de archivo proporciona el marco institucional necesario para desarrollar los

procedimientos que aseguren tal preservación. Basados en la infraestructura delineada en el Marco de Políticas desarrollado por InterPARES 2, la política y los procedimientos constituyen –juntos– un Programa de Preservación de Documentos Digitales de Archivo, que abarca la disposición de todos los documentos digitales de archivo del BCIT valorados para su mantenimiento a largo plazo; y de aquéllos valorados para su preservación permanente en el archivo.

Mandato

Se debe formular y promulgar una política por parte de la organización, la agencia o el departamento. La inclusión de un mandato indicará que el cuerpo regulador que la promulga tiene autoridad para hacerlo; las políticas dan soporte a las necesidades de negocio del departamento o la organización.

Ejemplo

cIRcle, Política de Adquisición.

cIRcle es el depósito digital de la Universidad de British Columbia (UBC) para los materiales de investigación y enseñanza creados por la comunidad de la UBC y sus socios. Los materiales de cIRcle son accesibles de manera abierta a través de su página web para cualquiera, tienen URL persistentes y serán preservados para generaciones futuras.

Declaración de política

Proporciona un marco que permite abordar la responsabilidad de los creadores de los documentos de archivo y asegura que éstos son creados fiables y se mantienen auténticos y exactos. Debería basarse en las necesidades de negocio de la organización, no en la tecnología utilizada para lograr esas necesidades.

Las políticas se revisarán periódicamente y se modificarán a medida que las necesidades de negocio evolucionen.

Ejemplo

Vancouver School of Theology (VST), Política de Administración de Archivos.

La VST reconoce que la administración eficaz de sus documentos de archivo, con independencia de su forma o soporte, es esencial para dar sustento al trabajo de la escuela, facilitar la gobernanza y la administración; y hacer posible el que cumpla con sus obligaciones legales y reguladoras. La VST está comprometida con el desarrollo de un programa eficaz de administración de archivos que promueva la accesibilidad del documento de archivo y dé soporte a la VST en lo concerniente a la satisfacción de sus obligaciones con respecto a la responsabilidad y la protección de la privacidad, reduciendo el riesgo y maximizando la eficacia.

Esta política proporciona un marco para la creación, administración y preservación permanente de los documentos de archivo de la VST, sobre cualquier soporte, que sean auténticos, fiables y accesibles para uso actual y futuro.

Roles y responsabilidades

Esta sección enlaza la responsabilidad de implantar la política con la estructura organizacional general. Identifica partes interesadas y asigna responsabilidades continuadas para asegurar que todos los niveles organizacionales se adhieren a la política. Es en esta sección donde se examina y se define el marco de responsabilidad, manteniendo y aclarando la diferencia, si es aplicable, entre ser responsable de acciones relativas a documentos digitales de archivo y ser responsable de que otros lleven a cabo acciones relativas a documentos digitales de archivo.

Vancouver School of Theology, Política de Administración de Archivos.

Director – Administración de archivos y privacidad (o persona designada):

- Incrementa la conciencia de los problemas de la administración de archivos con el personal y los administradores; por medio de un cuadro de clasificación de documentos de archivo y calendarios de retención y disposición, con independencia de su soporte.
- Identifica, con las aportaciones y previa consulta a los administradores, los documentos digitales de archivo ya existentes, asegura su carácter fidedigno de acuerdo con los "Requisitos de cota que dan soporte a la presunción de autenticidad de los documentos electrónicos de archivo" del Proyecto InterPARES 1; además, determina y mantiene sus relaciones con los correspondientes documentos de archivo en papel.
- Aconseja, forma y da soporte al personal en la implantación de procedimientos de administración de archivos.
- Trabaja con el director de TIC para seleccionar el hardware, el software y los formatos de fichero que ofrecen una mayor probabilidad de interoperabilidad y accesibilidad continuada a lo largo del tiempo.
- Supervisa el progreso de la implantación de procedimientos, proporcionando soporte y;
- Desarrolla, con las aportaciones de –previa consulta con– los administradores, según sea necesario.

Definiciones

Esta sección aporta un glosario de términos específicos del dominio o de la organización utilizado en la política, especialmente si el uso de esos términos difiere de la usanza en la lingua franca de la organización.

Ejemplos

Ejemplo 1. BCIT, Política de Preservación Digital.

Los documentos de archivo activos son los de uso actual, significando que se hace referencia a ellos al menos una vez al mes, por cada serie de documentos de archivo. Se almacenan en áreas de oficina y en servidores de tecnologías de la información que son inmediatamente accesibles.

Ejemplo 2. cIRcle, Política de Adquisiciones.

Preservación de bits: garantía de que los bits que conforman un objeto digital seguirán siendo los mismos a lo largo del tiempo, evitando la corrupción, la pérdida de datos y otros daños.

Comunidad: institución, facultad, departamento o grupo identificado que crea o genera materiales.

Fuentes relacionadas

Las políticas deben adherirse a las legislaciones relevantes tanto nacional como regional y puede seguir normas y buenas prácticas relevantes. Debería hacerse referencia a estas leyes, políticas, normas y buenas prácticas en la política, así como a las políticas organizacionales relacionadas.

Ejemplo

BCIT, Política de Preservación Digital.

Políticas del BCIT:

- 6700, Freedom of Information and Protection of Privacy.
- 6701, Records Management.
- 6702, Archives and Special Collections.

Legislación:

- BC Evidence Act
- BC Freedom of Information and Protection of Privacy Act
- Canada Copyright Act
- Canadian Patent Act
- Canadian Trade-Marks Act

Recomendaciones y normas:

- Canadian Digital Information Strategy (October 2008)
- Electronic Records as Documentary Evidence (CAN/CGSB-72.34-2005)
- Canadian General Standards Board Microfilm Standard

Control de versiones

Toda política debería contener información sobre el control de versiones para asegurarse de que todas las partes interesadas siguen las políticas más actualizadas. La información necesaria para dar soporte al control de versiones incluye:

- Número de versión de la política.
- Fecha en que la política es eficaz.
- Si la política ha sido sustituida, fecha en que la política ha sido sustituida.
- Cada política debe hacer referencia de las políticas a las que sustituye (si ha sido sustituida, referencia a la versión actualizada).

Revisión de la política

Las políticas deberían ser aprobadas por el nivel de gestión más alto que refleje la importancia del asunto. Puesto que los

documentos de archivo representan testimonio de las actividades de una organización y mantienen a ésta responsable de sus acciones, los altos niveles de gestión deberían aprobar una política de preservación digital. Si es necesario, la revisión de la política también debería buscar asesoramiento legal para asegurarse de que la política se adhiere a la legislación relevante y está armonizada con las políticas organizacionales relacionadas que regulan los documentos de archivo, el acceso a la información y la privacidad.

Las políticas deberían revisarse periódicamente, para asegurar que siguen proporcionando las mejores recomendaciones en consideración de los fines de la organización. La política debería identificar quién, cómo, cuándo y por quién será revisada la política misma (por ejemplo, debería existir un requisito en la política para que los gestores de negocio sean responsables de revisar la implantación de la política dentro de sus propias áreas). Como parte integrante de esta revisión periódica, esta sección también debería identificar quién, cómo, cuándo y por qué serán ejecutadas las auditorías y las evaluaciones de la implantación de la política.

Debe contener la siguiente información:

- El –o los– individuo(s) y el –o los– departamento(s) responsable(s) de aprobar la política.
- El lapso entre revisiones.
- La fecha en que la política fue revisada por última vez.
- La fecha en la que la política fue aprobada por el –o los– individuo(s) o departamento(s) relevante(s) y;
- La fecha de la siguiente revisión.

Fecha

clRcle, Política de Adquisiciones.

Esta política está sujeta a aprobación por la Biblioteca de la UBC y será revisada cada tres años. Como parte de la revisión, todas las referencias específicas a legislación, políticas u otros documentos deberían actualizarse para reflejar la última iteración de todos los materiales.

Caso de estudio: Desarrollo de una política en una institución técnica post-secundaria

En los ejemplos se presenta este caso de estudio para ilustrar la metodología presentada en este módulo, aplicada en una situación de la vida real. Está orientada a ayudar a comenzar el proceso de desarrollo de una política y a dar soporte a la experiencia de aprendizaje de este módulo. Puesto que cada organización es diferente y debemos aproximarnos a ella con una visión práctica de la implantación de los principios, es en la práctica real donde los retos a la metodología se revelan y resuelven.

Antecedentes acerca del Instituto

El Instituto se unió a InterPARES 3 (IP3) como un socio a prueba para desarrollar una política y unos procedimientos que estuvieran informados por ella; y que reflejaran investigación de última generación en la creación y mantenimiento de los documentos digitales de archivo.

El Instituto es una gran institución post-secundaria, con una matriculación anual de 16 mil estudiantes de tiempo completo y 32 mil estudiantes de tiempo parcial. La escuela ofrece certificados, diplomas y títulos de grado aplicados; y emplea a más de 2 mil académicos y personal de tiempo completo y

tiempo parcial. La educación se proporciona en seis escuelas (facultades) con clases y oficinas en cinco campus. Cuenta con un director asociado de Privacidad y Administración de Archivos.

Los documentos de archivo se crean en todos los departamentos y están sujetos al sistema de clasificación de la escuela y al Directorio de Documentos de Archivo. La clasificación está vinculada a los calendarios de retención y, aunque cada departamento designa administradores de documentos de archivo, el director asociado de Privacidad y Administración de Archivos tiene la superintendencia general sobre todas las funciones de administración de archivos. Este sistema funciona bien para documentos de archivo en formatos tradicionales (papel, microfilm y otros), pero es presionado por el creciente uso de computadoras personales y otras tecnologías digitales, para crear documentos de archivo.

Existen en uso varios sistemas de creación y almacenamiento de documentos de archivo para tipos específicos de documentos de archivo estructurados, pero los no estructurados se mantienen en bibliotecas de documentos digitales que son creados por el departamento de Tecnología de la Información a petición de departamentos individuales, generalmente sin consultar al director asociado, de Privacidad y Administración de Archivos.

Los documentos tradicionales de archivo estaban bien gestionados bajo varias políticas y procedimientos interrelacionados. Aunque en principio éstos regulaban todos los documentos de archivo con independencia del soporte, en realidad el tiempo había venido a actualizar las políticas y los procedimientos para cubrir los documentos digitales de archivo, para que estos importantes activos estuvieran sujetos a la misma responsabilidad que sus contrapartidas tradicionales.

El Instituto quería desarrollar políticas y procedimientos para la preservación de sus documentos digitales de archivo, la cual complementaría la ya existente y los procedimientos asociados expandirían los procedimientos para administración de archivos y reemplazarían la sección desfasada sobre documentos electrónicos de archivo en los procedimientos ya existentes. Esto tenía que ser presentado como una política para preservar documentos digitales de archivo. No abordaba, ni lo pretendía, la preservación archivística, sino la capacidad para crear, mantener y utilizar documentos digitales de archivo, auténticos, fiables y exactos, a lo largo de todo su ciclo de vida, mientras todavía estaban bajo la custodia del creador.

Los retos

El Instituto tiene dos políticas de administración de archivos (Administración de archivos; Archivos y colecciones especiales); y ha establecido procedimientos para asegurar la preservación de documentos analógicos de archivo. El Instituto tiene 100 millones de documentos digitales de archivo y, sin embargo, no cuenta con ninguna política ni con procedimientos en vigor para la preservación a largo plazo de documentos digitales de archivo, los cuales están sujetos a clasificación y retención, pero no están completamente implantados para los documentos digitales de archivo, como lo están sus homólogos analógicos y en película. Los documentos de archivo del Instituto están en peligro de pérdida debido a la obsolescencia tecnológica. Adicionalmente, los requisitos de la legislación de libertad de información (FOI) y privacidad requieren que el Instituto sea consciente de los documentos digitales de archivo de su posesión y de sus contenidos para proteger la información personal y hacer que los documentos de archivo relevantes estén disponibles bajo demanda a efectos de libertad de información. Actualmente, el Instituto tiene una cultura organizacional que no es consciente o comprensiva, de manera uniforme, en relación con los problemas de la administración de archivos.

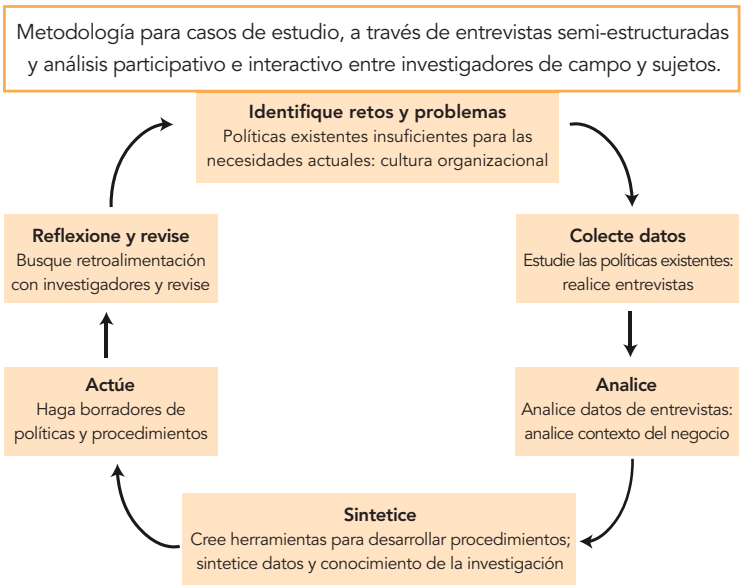


Figura 6

El proceso de desarrollo de políticas

- **Recopilación de datos (análisis contextual y cuestiones a investigar).** Los investigadores entrevistaron al personal de gestión y administrativo clave para construir el análisis contextual y responder a preguntas acerca de los documentos de archivo, los sistemas de gestión de documentos y el proceso de desarrollo de políticas del Instituto. Esto se ejecutó a un nivel alto, más que a nivel de procesos de creación de documentos individuales de archivo en departamentos individuales.
- **Revisión de las políticas ya existentes.** Los investigadores analizaron las políticas y los materiales de administración de archivos ya existentes, para

comprender las prácticas y la cultura de administración de archivos del instituto.

- Los investigadores **identificaron las normas y buenas prácticas relevantes** que tenían que tomarse en consideración.
- Los investigadores **identificaron los huecos en la política vigente** que tenían que ser abordados.
- Los investigadores **redactaron una política en armonía con la de administración de archivos vigente** (con otras políticas, como aquéllas de instituciones de libertad de información y de archivos); y añadieron responsabilidades a los distintos niveles de creadores de documentos de archivo y aquéllos con autoridad sobre los documentos de archivo, para asegurar que se satisfacían los retos planteados por la tecnología digital. Los investigadores y el Director Asociado de Privacidad y Administración de Archivos, del instituto; y exploraron los problemas relacionados que estaban conduciendo el desarrollo de esta política. Lo hicieron para identificar los huecos que tenían que abordarse.

Es importante hacer notar que este proceso no fue lineal. Mediante discusión y análisis por parte del director asociado de Privacidad y Administración de Archivos y los investigadores, fue un proceso iterativo el que condujo a la generación del borrador final de la política, que fue entonces presentado al órgano autorizado del Instituto. Una vez que la política estuvo aprobada, los investigadores comenzaron el proceso de desarrollar procedimientos que dieran soporte a la política.

Los procedimientos se desarrollaron siguiendo el mismo modelo. La diferencia en el proceso estuvo en el nivel de granularidad del detalle. Mientras que la política articula conceptos de alto nivel que delinean y guían las responsabilidades, los procedimientos

proporcionan a los creadores de documentos de archivo actividades y responsabilidades concretas para asegurar la creación de documentos de archivo, auténticos, fiables, exactos y utilizables.

Los investigadores entrevistaron a los administradores de archivo con responsabilidad directa sobre los documentos de archivo de sus departamentos. En el proceso de ejecución de las entrevistas, surgieron muchas cuestiones que alertaron a los administradores de archivo acerca de los riesgos inherentes a la continuidad del "negocio como es usual". Los ejemplos incluyen el aumento de la conciencia acerca del riesgo de mantener y almacenar documentos de archivo en formatos que no son fijos; y los riesgos de enviar por correo electrónico documentos de archivo sensibles a órganos de gobierno externo, que podrían no ejercer el mismo nivel de control que se aplicaba internamente.

Los investigadores establecieron una concordancia entre la práctica actual –tal y como fue obtenida de los datos de las entrevistas– y los actuales procedimientos escritos; y luego establecieron una concordancia entre estos datos y la nueva política. Con estas concordancias fueron capaces de redactar procedimientos que cerraban huecos y, si se seguían, asegurarían la creación y el mantenimiento de documentos de archivo auténticos, fiables, exactos y utilizables.

Cuestionamientos de revisión

Las siguientes preguntas se diseñaron para proporcionar a los lectores de este módulo la oportunidad de examinar algunos de los conceptos y las cuestiones, presentados de manera más estricta; y de evaluar el modo en que los conceptos presentados se aplican a su organización.

- Describa las diferencias clave entre políticas y procedimientos.

- Identifique el propósito y los componentes clave de un sistema de gestión de documentos digitales de archivo y de una política de preservación digital.
- ¿Cuáles son las ventajas y las desventajas de incluir la preservación en una política general de administración de archivos frente a tener una política separada de preservación digital?
- Identifique los principales principios en el desarrollo de una política de preservación digital.
- ¿Cuál es el papel de la política con respecto a la conformidad?
- ¿Qué papel juega la política de preservación digital en la libertad de información, el acceso y la privacidad; los litigios, el e-descubrimiento y la responsabilidad organizacional?

Ejercicios

Ejercicio 1: Análisis de política. Política de disposición de los documentos electrónicos de archivo de la universidad[2]

Utilizando lo que ya ha aprendido acerca del diseño de políticas eficaces, identifique las fortalezas y las debilidades de las siguientes políticas de muestra.

En particular, considere:

- ¿Qué información esencial de una política le parece que falta?
- ¿Qué información incluida en esta política podría situarse mejor en otros instrumentos de control (por ejemplo, recomendaciones, procedimientos y demás)?

[2] Véase el Apéndice G para algunos puntos de discusión sugeridos.

Política de disposición de documentos electrónicos de archivo de la Universidad

Propósito

- El propósito de esta política es asegurar que todos los documentos electrónicos de archivo de la Universidad son creados y mantenidos –y se accede a– y se dispone de ellos de manera controlada, por los siguientes motivos:
  - Dar soporte a las funciones de negocio de la Universidad y de sus partes interesadas.
  - Mantener evidencia a efectos de posible litigio, mediación, arbitraje o vistas disciplinarias.
  - Adherirse a la Política de Administración de Archivos de la Universidad.
  - Adherirse al Calendario de Retención de Documentos de Archivo de la Universidad.
  - Adherirse a la Provincial Universities Act.
  - Adherirse a la Access to Information Act.

Alcance

- Esta política se aplica a todos los documentos electrónicos de archivo creados, recibidos y mantenidos por la universidad.

Declaración de política

- La disposición de documentos electrónicos de archivo debe adherirse al Calendario de Retención de Documentos de Archivo de la Universidad.
- Los documentos electrónicos de archivo de los que se ha programado su destrucción, en la fecha definida pueden ser:

- Borrados, incluidas todas las copias mantenidas en todos los soportes (incluso la intranet de la universidad, equipos de trabajo del personal, unidades flash, CD, DVD y/o cualquier otro soporte externo).

- Todas las copias en papel de documentos electrónicos de archivo de los que se ha programado su destrucción serán:
  - Trituradas, si los documentos de archivo contienen información sensible o confidencial.
  - Recicladas, si los documentos de archivo no contienen información sensible o confidencial.
- Los documentos de archivo de los que se ha programado su retención permanente por el archivo deberán, en la fecha de transferencia, ser transferidos mediante uno de los siguientes métodos:
  - Ser colocados en el *Dropbox* del Archivo de la universidad en la intranet de la universidad.
  - Ser enviados por correo electrónico al Archivero de la universidad.
  - Ser entregados mediante un soporte de almacenamiento externo, incluidos dispositivos flash, CD o DVD.

Funciones y responsabilidades

- Archivero de la universidad:
  - El Archivero de la Universidad supervisa el Programa de Administración de Archivos de la universidad.
  - El Archivero de la universidad, de acuerdo con ésta y otras políticas aplicables, deberá:
    - Desarrollar revisar y actualizar periódicamente el Calendario de Retención de Documentos de Archivo de la universidad.

        - Asistir a los departamentos, los académicos y el personal de la universidad en la administración y disposición de sus documentos de archivo, mediante la provisión de documentos de recomendaciones y formación.
    - Crear procedimientos, tal y como se detalla en esta política.
- Empleados de la universidad:
    - Todos los empleados de la universidad crearán y mantendrán documentos de archivo, completos y exactos, para dar soporte a las funciones de negocio de la universidad.
    - Todos los empleados de la universidad asegurarán la disposición adecuada de los documentos electrónicos de archivo, de acuerdo con esta política y con todos los procedimientos relacionados con esta política.

Políticas y documentos de la universidad relacionados

- Política de administración de archivos de la universidad.
- Calendario de retención de documentos de archivo de la universidad.

Legislación relacionada

- *Provincial Universities Act.*
- *Access to Information Act.*

Revisión

- Esta política será revisada cada cinco años y debe ser aprobada por la Junta de Regentes de la universidad y el Consejo Legal de la universidad.

- Fecha de aprobación: 5 de marzo de 2010.
- Fecha de la siguiente revisión: marzo de 2012.

Ejercicio 2: Análisis y revisión de la política[3]

Utilizando lo que ha aprendido acerca del diseño eficaz de políticas, identifique las fortalezas y debilidades de la siguiente política de muestra que regula la administración, valoración y disposición de documentos digitales de archivo, para un archivo regional que tiene el mandato de preservar los documentos de archivo del gobierno local. Dentro de la región, existen diferentes organizaciones gubernamentales con diversos sistemas y niveles de competencia para administrar y preservar documentos digitales de archivo. El archivo proporciona asesoramiento y establece normas sobre la creación, administración y preservación de los documentos digitales de archivo de las agencias del gobierno; determina el valor archivístico de los documentos digitales de archivo; promulga autorizaciones de disposición para documentos digitales de archivo cuando ya no sirven a los requisitos legales, administrativos y de negocio de las agencias; y proporciona acceso público a los documentos digitales de archivo transferidos al archivo.

En particular, considere lo siguiente:

- ¿Cuáles son las fortalezas y las debilidades de la política? ¿Por qué?
- ¿Qué se ha perdido de la política?
- ¿Cuáles son las implicaciones de los elementos perdidos en términos de implantación de la política?

[3] Véase el Apéndice G para algunos puntos de discusión sugeridos.

- Discuta la idoneidad o falta de idoneidad de:
  - La sección de roles y responsabilidades de esta política.
  - La sección de definiciones de la política.
  - La declaración de alcance de esta política.

Política sobre la administración, valoración y disposición de documentos digitales de archivo

Objetivo

- Proporcionar un marco y una estrategia integrados para la administración, valoración y disposición de documentos digitales de archivo, fiables, exactos y auténticos, generados en los sistemas de información de negocio de las agencias públicas. Se aplica a los propietarios de los documentos de archivo, los administradores de TIC y los funcionarios o usuarios de las agencias públicas.

Definiciones

- A efectos de esta política, se aplican las siguientes definiciones:
  - *Documentos digitales de archivo.* Se refiere a los documentos de archivo, creados, recibidos, procesados y almacenados en forma electrónica o digital como los documentos de archivo oficiales y públicos de la agencia pública en el curso de transacciones de negocio oficiales por parte de los funcionarios de la agencia.
  - *Datos.* Se refiere a las representaciones electrónicas de la información (definiciones, cifras, informaciones o instrucciones), utilizadas para

comunicación y procesamiento por un sistema informático.

Roles y responsabilidades del personal en gestión de documentos

- La administración de documentos digitales de archivo es una responsabilidad compartida y requiere que las diversas partes interesadas trabajen en cooperación para asegurar que están en uso infraestructuras, sistemas y procedimientos, para cumplir con una buena gestión de documentos y buenas prácticas de preservación.
- Los propietarios de los documentos de archivo y los administradores de TIC son responsables de:
    - Desarrollar reglas y procesos de negocio para crear y capturar documentos digitales de archivo en sistemas de información de negocio y vincular metadatos a los documentos.
    - Alinear los procesos de TIC con los procedimientos de gestión de documentos, incluido el aseguramiento del uso adecuado, la retención, la disposición, la conversión y la migración de documentos digitales de archivo.
    - Implantar controles de acceso y medidas de seguridad.
    - Determinar durante cuánto tiempo deberían mantenerse los documentos de archivo (por ejemplo: periodo de retención), basándose en los procesos de negocio, el marco legislativo y los requisitos financieros.
    - Administrar los cambios en el sistema de gestión de documentos en relación con los cambios en los procesos y necesidades de negocio, las actualizaciones de *software* y las nuevas tecnologías.

Buenas prácticas en gestión de documentos

- Tener en vigor un sistema fiable de gestión de documentos, para administrar documentos digitales de archivo, de los cuales los correos electrónicos conforman una gran proporción. Es aconsejable que una organización invierta en un sistema fiable de gestión de documentos que ayude a asegurar que las decisiones gubernamentales importantes capturadas en correos electrónicos y formatos digitales se administran eficazmente y se salvaguardan para asegurar su responsabilidad, su carácter fidedigno y su fiabilidad, así como su accesibilidad a largo plazo.
- Asegurar que los documentos digitales de archivo y sus metadatos están integrados en el sistema. Los metadatos proporcionan información contextual para comprender cómo, cuándo, por qué y por quién fue creado y transmitido un documento de archivo. Son un componente esencial de una buena gestión de documentos. Los metadatos deberían capturarse primero en el punto en el que un documento es creado y capturarse periódicamente a medida que tengan lugar más acciones sobre los documentos de archivo. Las pistas de auditoría son un tipo de metadatos y proporcionan información contextual e historia sobre la creación y el uso de los documentos de archivo dentro del sistema. Por ejemplo, cuándo fue creado un documento de archivo, en qué momento se accedió a él, cuándo fue editado y por quién.

Valoración de documentos digitales de archivo

- Objetivo de la valoración:
  La valoración oportuna de los documentos digitales de archivo asegura la identificación, la salvaguarda

y la protección adecuadas de los documentos de archivo de los que se considera que tienen un valor de negocio continuado, identificados para su preservación a largo plazo, o que tienen valor archivístico.

- Cuándo valorar:
  - Idealmente, la necesidad de la preservación digital debería identificarse en la fase de planificación, y los documentos digitales de archivo deberían ser valorados durante la fase de diseño e implantación del sistema para facilitar el proceso de integrar las funcionalidades de gestión de documentos y de preservación, y para asegurar que las acciones de valoración y de disposición están incorporadas al sistema.
  - Las decisiones de valoración deberían revisarse periódicamente, porque a lo largo del tiempo los procesos de negocio pueden cambiar y los sistemas de gestión de documentos pueden evolucionar. Como tales, tanto la agencia de creación o transferencia, como el archivo, tienen que supervisor y revisar las anteriores decisiones de valoración.

Destrucción de documentos digitales de archivo de valor a corto plazo o transitorio

- Los documentos digitales de archivo que tienen valor a corto plazo y transitorio, como los documentos de archivo de los que se entiende que dan soporte a actividades de gestión interna –por ejemplo, una solicitud de licencia y el pago financiero–, pueden destruirse de manera rutinaria de conformidad con el *Calendario general de retención de documentos electrónicos de archivo*.

Transferencia de los documentos digitales de archivo, ya valorados, al archivo provincial para su preservación a largo plazo

- Las agencias son responsables de la autenticidad y fiabilidad de los documentos digitales de archivo que crean y transfieren al archivo regional para su preservación permanente.
- Las agencias deberían desencriptar y descomprimir los documentos digitales de archivo antes de enviar los que tienen valor archivístico al archivo provincial. El uso de tecnologías de autenticación como las firmas digitales asegura la integridad de los datos y confirma la identidad del remitente en un punto específico del tiempo, aunque no es suficiente para asegurar la integridad y la preservación de los documentos electrónicos de archivo a lo largo del tiempo.

Recursos

Existen muchos excelentes recursos disponibles para el desarrollo de políticas que regulen el mantenimiento y la preservación de documentos digitales de archivo. La siguiente lista no es –ni pretende ser– exhaustiva, sino que está orientada a ofrecer una selección de recursos disponibles. Se han elegido porque son obras seminales en este campo, ofrecen los resultados de influyentes investigaciones originales y reflejan el conocimiento colectivo de "buenas prácticas", a partir de un área disciplinar o una comunidad de práctica particulares. Muchas de las fuentes listadas aquí también incluyen bibliografías que conducirán al lector a una red más amplia de recursos.

Autor: ARMA International (Asociation of Record Managers and Administrators), y Society of American Archivists (SAA).

Título: *Sample Forms for Archival & Records Management Programs.*

Detalles de la publicación: 2002.

Editor: Lenexa, KS: ARMA International.

Este recurso contiene aproximadamente 200 formularios y políticas de muestra que los usuarios pueden personalizar para adecuarlos a las necesidades de su organización. Los formularios incluidos cubren funciones de administración de archivos y archivísticas, incluidos el inventario y la programación; la destrucción y la disposición de documentos de archivo; la auditoría; la valoración; la ordenación y la descripción; entre otras. Los formularios se incluyen en el recurso en copia impresa y a los usuarios se les da acceso a las versiones electrónicas de los formularios, los cuales pueden descargarse y personalizarse para adecuarse a las necesidades de la organización. Existe un costo para este recurso.

Autores: Shepherd, Elizabeth y Geoffrey Yeo.

Título: *Managing Records: A Handbook of Principles and Practice* (Chapter 8: Implementing Records Management: Practical and Managerial Issues).

Detalles de publicación: 2003.

Editor: Londres: Facet Publishing.

Este libro es un texto comprehensivo que delinea los principios de la administración de archivos y su implantación práctica en las organizaciones. Es comprensivo en su cobertura de los conceptos, prácticas y problemas de la administración de archivos. Es útil tanto para los recién llegados a la profesión como para administradores de archivos más experimentados;

los asuntos cubiertos incluyen el contexto organizacional; la clasificación; la creación y la captura de los documentos de archivo; la valoración, la retención y la disposición; el acceso y la implantación. El libro incluye una bibliografía comprehensiva de recursos en administración de archivos así como listas de normas de administración de archivos y organizaciones profesionales, para administradores de archivos nacionales e internacionales.

Autor: International Organization for Standardization (ISO).

Título: *Information and Documentation. Records Management.*

Detalles: ISO 15489-1: 2001, Part 1: Section 6; Part 2: Sections 2 and 3.2.6.

Editor: ISO.

La Organización Internacional de Normalización (ISO), es una federación internacional de órganos nacionales de normalización que prepara y publica normas internacionales. Los comités técnicos de ISO están compuestos por representantes de los órganos miembros, así como de organizaciones internacionales. Y los órganos gubernamentales y no gubernamentales preparan las normas ISO 15489 consta de las siguientes partes, bajo el título general *Information and Documentation: Records Management: Part 1: General, and Part 2: Guidelines* [Informe técnico]. ISO 15489 fue desarrollada en respuesta al consenso entre los países miembros de ISO participantes, para normalizar buenas prácticas internacionales en administración de archivos utilizando las normas australianas AS 4390, *Records Management* como su punto de partida. ISO 15489 proporciona recomendaciones acerca de una administración eficaz de archivos dentro de las organizaciones, para asegurar que se preste la atención y la protección adecuadas a todos los documentos de archivo;

y que la evidencia y la información que contienen pueden recuperarse de manera más eficiente y eficaz, utilizando prácticas y procedimientos normalizados.

Autor: The National Archives (TNA).

Título: *How to Produce a Corporate Policy on Electronic Records.*

Detalles de publicación: septiembre de 2000, versión 1.

Editor: Crown, Public Records Office.

URL: http://www.nationalarchives.gov.uk/documents/rm_corp_pol.pdf

Este informe, desarrollado por el Archivo Nacional del Reino Unido, está orientado a facilitar el desarrollo de una política por parte de los Funcionarios Departamentales de Documentos de Archivo (DRO), dentro de sus propios departamentos y agencias. Aunque orientado a los DRO, es un recurso útil para cualquier personal al que se le hayan asignado responsabilidades en administración de archivos, incluido el desarrollo de políticas. El informe proporciona recomendaciones sobre la planificación, qué debería cubrir una política, la importancia y la incorporación de un marco de políticas, la implantación y la auditoría. Delinea los diversos componentes esenciales para una política organizacional eficaz sobre documentos electrónicos de archivo, delineando principios genéricos que pueden aplicarse a la administración de documentos electrónicos de archivo.

Autor: TNA.

Título: *Digital Preservation Policies: Guidance for Archives.*

Detalles de publicación: 2011.

Editor: Crown, Public Records Office.

URL: http://www.nationalarchives.gov.uk/documents/digital-preservation-policiesguidance-draft-v4.2.pdf

Esta guía fue desarrollada por el Archivo Nacional de Reino Unido para proporcionar recomendaciones a archivos de financiación pública sobre el desarrollo de políticas de preservación digital. La guía delinea las características clave de una política de preservación digital y discute por qué es necesaria, así como el modo en que una política da soporte a la preservación digital. La guía está orientada a ayudar a las organizaciones a mejorar la gobernanza de la preservación digital por medio del desarrollo de una política de preservación digital. Aunque esta guía está dirigida a archivos de financiación pública, otros archivos pueden encontrar esta guía útil en el desarrollo de una política de preservación digital.

Autor: Beagrie, Najla Semple, Peter Williams, Richard Wright.

Título: *Digital Preservation Policies Study.*

Preparado por: Charles Beagrie Limited.

Detalles de publicación: HEFCE 2008, Part 1: Final Report, octubre de 2008.

Editor: Joint Information Systems Committee (JISC).

URL: http://www.jisc.ac.uk/media/documents/programmes/preservation/jiscpolicy_p1final report.pdf

Este informe –financiado por el JISC– es resultado de un reporte que pretendía proporcionar conocimiento en la función de la preservación digital, en soporte de estrategias clave en el

entorno de la educación superior en Reino Unido; y crear un modelo de políticas de preservación digital para instituciones de educación superior del Reino Unido. La publicación consta de dos herramientas: 1) un modelo y marco para una política de preservación digital y cláusulas de implantación basadas en el examen de las políticas de preservación digital ya existentes; 2) una serie de concordancias entre enlaces de preservación digital a otras estrategias institucionales clave en universidades y escuelas de Reino Unido. El informe sirve como guía práctica para desarrollar una política de preservación digital institucional. Contiene consejos sobre política estratégica, apoyados por secciones adicionales de lecturas que seleccionan y proporcionan breves descripciones de recursos clave ya existentes, para ayudar en la implantación utilizando estrategias y herramientas específicas.

Autor: The State Records Authority, New South Wales (SRNSW).

Título: *Examples of Policy, Procedure and Planning.*

Preparado por: State Archives.

Detalles de publicación: 2010.

Editor: Department of Services, Technology & Administration

URL: http://www.records.nsw.gov.au/recordkeeping/useful-resources/examples-of-policy-procedure-and-planning/examples-of-policy-procedure-and-planning

La State Records Authority of New South Wales administra los archivos de NSW, establece las reglas y proporciona recomendaciones sobre la administración de documentos oficiales de archivo. Administra un marco de política, legislación, normas, códigos de buenas prácticas y recomendaciones que regulan

la creación, el mantenimiento, la preservación de –y el acceso a– documentos de archivo del sector público y fondos de archivo. Entre sus útiles e informativas páginas Web está la de recursos que ofrece ejemplos de política, procedimientos y planificación. Los ejemplos incluyen políticas sobre administración de archivos, dispositivos de comunicación, disposición de documentos de archivo con imágenes, y planes estratégicos y operativos.

Autor: Electronic Resource Preservation and Access Network.

Título: *Digital Preservation Policy Tool.*

Detalles de publicación: septiembre de 2003.

Editor: Information Society Technologies.

URL: http://www.erpanet.org/guidance/docs/ERPANETPolicyTool.pdf

Esta herramienta expone los motivos para desarrollar una política de preservación digital, las ventajas de tener una, los elementos a ser incluidos en ella, problemas, y otros aspectos específicos y relevantes. Examina políticas en uso o en desarrollo para preservar y mantener materiales digitales, fijándose, en particular, en aspectos específicos, como costes, requisitos, roles, responsabilidades, supervisión y revisión. Incluye una bibliografía de recursos sobre políticas de preservación digital, con un enfoque en las bibliotecas, los archivos universitarios y los documentos públicos de archivo de Reino Unido, Australia y Estados Unidos.

Autor: The InterPARES 2 Project, Luciana Duranti y Randy Preston (eds.).

Redactores: Luciana Duranti, Jim Suderman, Malcolm Todd.

Título: "A Framework of Principles for the Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records", en International Research on Permanent Authentic Records in Electronic Systems (InterPARES 2): Experiential, Interactive and Dynamic Records.

Detalles de publicación: Padova, Italy: Associazione Nazionale Archivistica Italiana, 2008.

URL: http://www.Interpares.org/ip2/display_file.cfm?doc=ip2_book_appendix_19.pdf

El *InterPARES Framework of Principles for the Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records* se basa en los resultados de la investigación sobre la capacidad para preservar documentos digitales de archivo fidedignos, lo que depende de las acciones emprendidas en el momento de su creación. El marco de InterPARES establece principios para guiar el desarrollo de políticas, estrategias y normas que sean lo suficientemente flexibles como para ser útiles en diferentes entornos nacionales, pero lo suficientemente coherentes para ser adoptadas por completo. Consta de 13 declaraciones de principios para los creadores de los documentos de archivo, listadas en orden de importancia relativa e indicadas como requeridas o recomendadas; y 13 declaraciones de principio para los preservadores de los documentos de archivo, listadas de manera similar. Las declaraciones del creador y del preservador tienen referencias cruzadas.

Autor: The Northeast Document Conservation Center (NEDCC).

Título: *Digital Preservation Template.*

Detalles de publicación: enero de 2007 (última revisión en octubre de 2007).

Editor: Interuniversity Consortium for Political and Social Research (ICPSR)

URL: http://www.nedcc.org/resources/soda/downloads/SoDAExerciseToolkit.pdf

Autor: Cornell University Library.

Título: *Cornell University Library Digital Preservation Policy Framework.*

Fecha de publicación: diciembre de 2004.

URL: http://commondepository.library.cornell.edu/cul-dp-framework.pdf

Este documento formaliza el marco en el que los activos digitales se identifican y aseguran para su preservación a largo plazo y acceso permanente. El programa de preservación –regulado por este marco– cumple con el Modelo de Referencia Open Archival Information System (OAIS). E incluye los principios de funcionamiento, las funciones, las responsabilidades, el alcance y los retos.

Autor: Library of Congress National Digital Information Infrastructure and Information Preservation Program.

Título: *Sustainability of Digital Formats: Planning for Library of Congress Collections.*

Fecha de publicación: 2007.

URL: http://www.digitalpreservation.gov/formats/sustain/sustain.shtml.

Este artículo delinea 7 factores de sostenibilidad para ser considerados cuando se eligen formatos digitales para cualquier

categoría de información, con el propósito de preservar información digital como un recurso para generaciones futuras. Influyen en la viabilidad y el coste de la preservación; y son significativos, con independencia de las estrategias de preservación elegidas.

Autor: National Library of Australia.

Título: *Digital Preservation Policy.*

Fecha de publicación: octubre de 2007.

URL: http://www.nla.gov.au/policy/digpres.html

Esta política refleja el compromiso de la Biblioteca Nacional de Australia de priorizar la accesibilidad permanente de sus recursos digitales, participar en la investigación, en la preservación digital, en el desarrollo de normas y trabajar con socios nacionales e internacionales para fomentar la preservación digital.

Autor: University of Illinois at Urbana-Champaign.

Título: *IDEALS Digital Preservation Policy.*

Fecha de publicación: octubre de 2007.

URL: https://services.ideals.uiuc.edu/wiki/bin/view/IDEALS/IDEALSDigitalPreservationPolicy

La iniciativa IDEALS trata de cumplir con la norma del Modelo de Referencia Open Archival Information System y con los requisitos de certificación para un Depósito Digital Seguro. La política de preservación digital asegura la recolección, la preservación y el acceso sostenible a los resultados académicos y de investigación de la universidad. La política compromete a la universidad

con la preservación dentro de un marco flexible que acomoda el desarrollo tecnológico.

Autor: Yale University Library.

Título: *Policy for Digital Preservation.*

Fecha de publicación: noviembre de 2005, actualizada en febrero de 2007.

URL: http://www.library.yale.edu/iac/DPC/revpolicy2-19-07.pdf

Este es un ejemplo de una política de preservación digital en el contexto de una importante biblioteca de investigación. La Biblioteca de la Universidad de Yale da soporte a la preservación física e intelectual; y a la estabilización técnica de recursos digitales a lo largo del tiempo, para asegurar el acceso permanente y mantener la autenticidad. Los elementos clave de la política reconocen que la capacidad para preservar recursos digitales y los costes implicados dependen de las decisiones adoptadas en todas las etapas del ciclo de vida de los documentos de archivo.

Apéndice A: Análisis contextual

Un análisis contextual así reúne datos acerca de la organización que influirán en la creación de políticas y procedimientos. Incluye información acerca de la estructura administrativa de la organización; sus obligaciones legales y reguladoras con respecto a sus documentos de archivo; pautas y normas que influyen en la creación, mantenimiento y uso del documento de archivo; los requisitos y restricciones de creación y gestión de documentos de archivo, incluidas la cultura de negocio de la organización, las restricciones de personal y las restricciones tecnológicas. Y proporciona la siguiente información:

Posición legal y reguladora

Identifique y proporcione información acerca de todas las leyes y regulaciones; y normas o códigos de conducta, legalmente requeridos, que regulen o afecten a la creación y gestión de documentos de archivo de su organización, incluidos los requisitos de retención y disposición.

Pautas

Identifique y proporcione información acerca de cualquier norma, metodología, código o regulación no requeridos legalmente, que regulen o afecten a la creación y gestión de los documentos de archivo de su organización, incluidos los requisitos de retención y disposición.

Recursos (físicos)

Resuma la información acerca del contexto físico en el que su organización funciona, incluyendo los datos relevantes acerca de equipamiento e infraestructura.

Gobernanza

Documente la estructura de gobernanza de su organización y el proceso de toma de decisiones en lo que se relacione con la administración de archivos.

Proporcione la(s) declaración(es) de misión, que puede(n) haber evolucionado a lo largo del tiempo.

Políticas

Identifique y proporcione información acerca de todas las políticas ya existentes que pertenezcan a los documentos de archivo, su creación, mantenimiento, retención y disposición y preservación a largo plazo.

Funciones

Liste todas las funciones principales que su organización emprende y que dan como resultado la creación de documentos de archivo.

Apéndice B: Análisis de los documentos de archivo. Prácticas actuales

Actividades que generan documentos y documentos de archivo

- Liste los tipos generales de actividades dentro de las funciones de su organización que dan como resultado la producción de documentos o documentos de archivo.
- Identifique a los creadores de documentos de archivo.

Documentos y documentos de archivo resultantes de las actividades

- Liste los principales tipos de documentos y documentos de archivo resultantes de estas actividades.

Existencia de un programa de administración de archivos

- Describa las actividades actualmente emprendidas que se relacionen con la administración de archivos.
- Analice cualquier política que el creador pudiera tener que regule la creación y administración de documentos de archivo.

Individuos responsables del mantenimiento de documentos de archivo

- Identifique el o los individuos responsables de mantener documentos de archivo después de su creación (mantenimiento de documentos de archivo). Éstos podrían ser designados del

personal de documentos de archivo, puede que sean los creadores de los documentos de archivo o ambos.

Existencia de estrategias de mantenimiento

Identifique el complejo de medios prácticos, formalmente articulados o informalmente implantados, que constituyen la administración de archivos. Esto incluye:

- La localización en la que los documentos de archivo se mantienen.
- El soporte o los medios en que los documentos de archivo se mantienen.
- Una descripción del modo en que están organizados los documentos de archivo.
- Una breve descripción de cualquier método utilizado para mantener documentos de archivo.
- Una breve descripción de cualquier método utilizado para intentar evitar la obsolescencia tecnológica mientras que los documentos de archivo están todavía activos o semiactivos.

Requisitos y restricciones tecnológicos

- Identifique y describa el equipamiento utilizado en su organización:
  - Arquitectura (por ejemplo, topología de redes, infraestructura, *hardware*).
  - Herramientas de creación o entrada (por ejemplo, *software*, cámaras, micrófonos),
  - Herramientas de procesamiento (por ejemplo, *software*, consolas).
- Identifique y describa los tipos de medios creados (por ejemplo, gráfico, textual, audio).

- Liste los formatos creados (por ejemplo, .pdf, .doc, .jpg) e identifique cualquier reto en particular relacionado con su mantenimiento y preservación.
- Identifique y describa el modo en que los requisitos o las restricciones tecnológicos relevantes tienen impacto sobre la creación, la forma, el contenido, la identidad, la integridad, la organización y la preservación de los documentos de archivo.

Si aplica: Requisitos y restricciones científicos

Son los fundamentos científicos de la disciplina con la que su organización se identifique y que requieran, influyan en, o prohíban, ciertas conductas.

- Identifique y describa el modo en que los requisitos o las restricciones científicas relevantes tienen impacto sobre las políticas y los procedimientos mediante los cuales se llevan a cabo las actividades.
- Identifique y describa el modo en que los requisitos o las restricciones científicas relevantes tienen impacto sobre la creación, la forma, el contenido, la identidad, la integridad, la organización y la preservación de los documentos de archivo resultantes de esas actividades.

Requisitos y restricciones artísticos

Son los principios o escuelas de pensamiento artísticos con los que su organización se identifica y que requieren, influyen en, o prohíben, ciertas conductas.

- Identifique y describa el modo en que los requisitos o las restricciones artísticos relevantes tienen

impacto sobre las políticas y los procedimientos mediante los que se llevan a cabo actividades.

- Identifique y describa el modo en que los requisitos o las restricciones artísticos relevantes tienen impacto sobre la creación, la forma, el contenido, la identidad, la integridad, la organización y la preservación de los documentos de archivo resultantes de esas actividades.

Apéndice C: Recomendaciones para el creador. Crear y mantener materiales digitales: recomendaciones para individuos[4]

Introducción

Hoy en día, la mayoría de la información se crea y almacena de forma digital. Las ventajas del soporte digital son, por ahora, familiares a todos. Los documentos pueden crearse rápidamente, editarse y revisarse con facilidad. Gracias a la Internet, pueden distribuirse globalmente a gran velocidad. Pueden manipularse de maneras que permiten que sean utilizados para múltiples propósitos. El soporte digital también resuelve los antiguos problemas de almacenamiento asociados con grandes ficheros de documentos de archivo en papel.

Las bendiciones de la era digital, sin embargo, no vienen sin costos. Sólo en años recientes la gente ha comenzado a comprender completamente los problemas inherentes al soporte digital. Por ejemplo, existe el hecho de que sólo puede accederse a la información digital utilizando una computadora que, además, debe tener el *software* necesario para ser capaz de leer las secuencias de bits contenidas en el disco o la cinta. La facilidad de reproducción y la proliferación de copias hace más difícil identificar la versión completa o final de un documento digital. La fácil distribución de información en internet hace más difícil la preservación de los derechos de propiedad intelectual. Finalmente, todos los materiales digitales son vulnerables a virus y a una simple falla tecnológica, así como a los

[4] Estas recomendaciones también han sido publicadas en forma de folleto ilustrado que está disponible en: http://www.interpares.org/display_file.cfm?doc=ip2(pub)creator_guidelines_booklet.pdf. Por favor, note que estas recomendaciones han sido incluidas aquí directamente desde el sitio Web de InterPARES –los apéndices a los que se hace referencia en estas *Recomendaciones* se refieren al libro IP2– esto se aclarará y fijará cuando el método final de distribución y su contenido se aprueben.

rápidos desarrollos de *software* y *hardware*, que los ponen en riesgo de hacerlos inaccesibles rápidamente.

Con todos estos problemas, no hay que asombrarse de que algunas personas supliquen por lo tangible y confortable del papel. Con todo, aunque es probable que nuestros sistemas para crear y mantener información sigan siendo –durante algún tiempo– sistemas híbridos. Esto es, contendrán tanto papel como materiales digitales, claramente, aunque no hay vuelta atrás en la revolución digital. En consecuencia, todos deberíamos ser conscientes de los riesgos a los que nos enfrentamos con los materiales digitales y aprender cómo minimizar, de la mejor manera, estos riesgos.

Estas recomendaciones han sido desarrolladas para individuos que crean materiales digitales en el curso de sus actividades profesionales y personales, para ayudarles a tomar decisiones informadas acerca de la creación y el mantenimiento de estos materiales, de manera que les ayuden a asegurar su preservación durante tanto tiempo como se necesiten. También pueden ser útiles para organizaciones pequeñas o grupos de individuos, como clínicas médicas, grupos de consultoría o equipos de investigación científica.

Aunque estas recomendaciones pueden aplicarse a distintos tipos de publicaciones, documentos y datos digitales, son especialmente importantes para los documentos digitales de archivo, que el usuario crea, recibe y utiliza en el curso de sus actividades; que mantiene porque puede necesitarlos más tarde o porque quiere tener evidencia fiable de lo que ha hecho. Por tanto, se tiene que ser especialmente cuidadoso en su mantenimiento y preservación. Estas recomendaciones son igualmente aplicables a documentos de archivo que tienen que mantenerse sólo por un breve periodo, como a aquéllos que requieren mantenimiento a largo plazo. La adhesión a estas

recomendaciones le ayudará a asegurar que los documentos de archivo que merecen preservación a largo plazo en un depósito archivístico, serán accesibles cuando pasen al cuidado de un custodio fiable.

Definiciones

Antes de presentarle las recomendaciones para guiarle en la creación y el mantenimiento de materiales digitales, será tanto necesario como útil aclarar el significado de algunos de los términos utilizados en este documento.

Para los fines de estas recomendaciones, un documento de archivo se define como cualquier documento creado (realizado o recibido y guardado, para posterior acción o referencia), por una persona física o jurídica en el curso de una actividad práctica como instrumento y resultado de esa actividad. Una publicación se define como un documento orientado a su diseminación o distribución al público en general. Todos los documentos de archivo y las publicaciones son documentos y contienen datos. Un documento es información asentada a un soporte en una forma fija; la información es un ensamblaje de datos orientados a su comunicación en el tiempo y el espacio; y los datos son piezas de información mínimas significativas e indivisibles.

Estas recomendaciones tratan de proporcionar indicaciones para la creación y el mantenimiento de materiales digitales fiables en general; y de documentos de archivo en particular, que puedan mantenerse y preservarse de manera exacta y auténtica a lo largo del tiempo. Para facilitar su aplicación, sin embargo, tienen que definirse los términos "fiabilidad", "exactitud", "autenticidad" y "autenticación".

Fiabilidad es el carácter fidedigno de los materiales digitales como declaraciones de hechos o como contenido. Es

responsabilidad del autor de los materiales –sea autor un individuo o la persona jurídica en cuyo nombre está escribiendo un individuo–, y se pondera sobre la base de la completitud y exactitud de los materiales y del grado de control ejercido en el proceso de su creación.

Exactitud es el grado en que los datos de los materiales son precisos, correctos, veraces y libres de error o distorsión. Para asegurarla, se debe ejercer control sobre los procesos de creación, transmisión, mantenimiento y preservación de los materiales. A lo largo del tiempo, la responsabilidad sobre la exactitud se desplaza desde el autor al gestor de los materiales y, posteriormente, al preservador a largo plazo de ellos (si resulta aplicable).

Autenticidad se refiere al hecho de que los materiales son lo que pretenden ser y no han sido manipulados ni corrompidos de ninguna otra manera. Así, con respecto a los documentos de archivo en particular, la autenticidad se refiere al carácter fidedigno en cuanto a documentos de archivo. Para asegurar que esa autenticidad puede presumirse y mantenerse a lo largo del tiempo, uno debe definir y mantener la identidad de los materiales y proteger su integridad. La autenticidad está en riesgo siempre que los materiales se transmiten en el espacio y en el tiempo. A lo largo del tiempo, la responsabilidad sobre la autenticidad se desplaza desde el gestor al preservador a largo plazo de los materiales.

Autenticación es una declaración de autenticidad, resultante de la inserción o de la adición de elementos o declaraciones a los materiales en cuestión; y de que las reglas que la gobiernan están establecidas por la legislación. Así, es un medio para probar que los materiales son lo que pretenden ser en un momento determinado. Las medidas de autenticación digital, como el uso de firmas digitales, sólo aseguran que los materiales

son auténticos cuando se reciben y no pueden ser repudiados. Sin embargo, no garantizan que seguirán siendo auténticos en lo sucesivo.

Recomendaciones

1. Seleccione *hardware*, *software* y formatos de fichero que ofrezcan la mejor esperanza para asegurar que los materiales digitales seguirán siendo fácilmente accesibles a lo largo del tiempo

Acceder a los materiales digitales depende de tener el *software* adecuado. El *software* que no es compatible con versiones anteriores (compatibilidad retrospectiva), o con futuras versiones (compatibilidad prospectiva), hace difícil acceder a los documentos de archivo a lo largo del tiempo. El *software* para una aplicación también tiene que funcionar bien con el de otras aplicaciones y sistemas (interoperabilidad). Prestar atención a los siguientes factores puede ayudar a asegurar que su *software* y su *hardware* mantienen la accesibilidad.

Elija software *que permita presentar los materiales tal y como aparecían originalmente.* Idealmente, los materiales deberían mantener la misma apariencia a lo largo del tiempo para ser completamente inteligibles y accesibles. Asegúrese de que el nuevo *software* será capaz de leer sus antiguos materiales en el formato que los gestionó y visualizó en pantalla, con la misma forma documental en la que originalmente se representaron. En otras palabras, el nuevo *software* debería ser retrospectivamente compatible con el *software* antiguo.

Elija software *y* hardware *que le permita compartir fácilmente materiales digitales.* El *software* debería ser capaz de aceptar y dar como salida ficheros en un cierto número de formatos diferentes. La capacidad para interactuar fácilmente con otra

tecnología se llama *interoperabilidad*. Esto hará más fácil acceder a sus materiales y también moverlos a otros sistemas.

Utilice software *que se adhiera a normas.* Ésta es una de las mejores cosas que puede hacer para asegurar que sus materiales durarán. Las normas aprobadas por organizaciones nacionales e internacionales son mejores. Se llaman normas de *jure*.[5] Si no existen para sus materiales, puede ayudar a asegurar la longevidad adoptar software que se utilice de manera muy general. En ausencia de una norma oficial, a menudo se hace referencia a este *software* como una norma *de facto*.[6] El *software* de fuente abierta, esto es, el *software* libremente disponible y no propietario, es preferible (véase subsección G).

Mantenga las especificaciones de software. Este tipo de documentación (por ejemplo, los manuales del propietario o cualquier otra descripción más detallada del *software* que pudiera tener), será esencial en el futuro para acceder a los materiales o para migrarlos a un nuevo entorno informático a medida que la tecnología avance. Es particularmente importante documentar por completo cualquier software que el usuario construya.

Si personaliza el *software*, asegúrese de que documenta los cambios que hace. Proporcione información detallada acerca de los cambios y describa claramente las características y los rasgos del material que los cambios producen, así como los resultados que está tratando de lograr al personalizar el *software*. Una

[5] Definida como una norma adoptada por un órgano oficial de establecimiento de normas, ya sea nacional (por ejemplo, ANSI), sea multinacional (por ejemplo, CEN) o internacional (por ejemplo, ISO). Para formatos de ficheros informáticos, dos recientes normas de jure son PDF/A (norma PDF para archivado) y ODF (OASIS Open Document Format).

[6] Definida como una norma no adoptada por ningún órgano oficial de establecimiento de normas, no obstante ser ampliamente utilizada y reconocida por sus usuarios como una norma. Bien conocidos y ampliamente utilizados formatos de ficheros informáticos que se consideran normas de facto incluyen PDF, TIFF, DOC y ZIP.

buena manera de hacer esto es incluir la información como comentarios en el código del *software*. La información no se perderá, porque es parte del fichero y será muy útil para aquellos que tengan que hacer ajustes posteriormente, a medida que la tecnología avance.

Documente la construcción de su sistema como un todo para ayudar a asegurar su accesibilidad. Documente la estructura y las funciones de su sistema. Esto significa identificar sus componentes de *hardware* y de *software*, incluidos periféricos; su sistema operativo y sus paquetes de *software*. Tal documentación identificará el modo en que los paquetes de *software* representan la información y el modo en que la procesan y comunican unos con otros y con los usuarios. Estas especificaciones básicas asegurarán que aquellos que vengan detrás comprenderán el contexto en el que se está trabajando ahora y proporcionarán la información necesaria para actualizar el sistema a medida que el *hardware* y el *software* evolucionen.

Elija formatos ampliamente utilizados, no propietarios, independientes de la plataforma, no comprimidos, con especificaciones libremente disponibles, siempre que sea posible. A menudo se les llama "formatos abiertos", lo que significa que su especificación está publicada y están disponibles.[7] Sin embargo, también puede significar que el formato está libre de patentes o regalías, o de la posibilidad de que tales tasas se apliquen en el futuro y/o que ha sido ampliamente adoptado. Debería hacerse notar que los formatos "abiertos" no son necesariamente lo mismo que los formatos producidos por *software de fuente abierta*, porque este último término describe *software* para el cual el código se ha hecho libremente disponible y puede modificarse. El *software* de fuente abierta no siempre produce formatos no propietarios. Distinga entre formatos de fichero, formatos envoltorio

[7] N. del E. Libre para consulta.

(o contenedor) y formatos etiquetados como ficheros etiquetados en XML; y asegúrese de que la versión, la codificación y otras características son claras y están completamente especificadas. Para los ficheros XML, asegúrese de que los ficheros están bien formados y son válidos; y vienen acompañados por las DTD o los esquemas relevantes. Si no es conveniente seguir esta recomendación, consulte con un archivo que acepte materiales digitales y elija entre los formatos que recomienda para preservación a largo plazo. No debería comprimir sus materiales digitales, si es posible, dado que esto puede conducir a problemas para su preservación a largo plazo. Si necesita comprimirlos, elija técnicas de compresión sin pérdida que se ajusten con las normas con normas internacionales aceptadas.

2. Asegúrese de que los materiales digitales mantenidos como documentos de archivo son estables y fijos tanto en su contenido como en su forma

Una de las grandes ventajas de los materiales digitales es la facilidad con la que la información puede editarse, revisarse o actualizarse. Sin embargo, esto también significa que información importante puede cambiarse o incluso perderse, accidentalmente o a propósito. Éste es un problema particularmente importante para los documentos de archivo, porque una de las características es que su contenido permanezca sin cambios y no se pueda modificar. Esto implica que la información y los datos del documento de archivo no puedan sobrescribirse, alterarse, expandirse ni borrarse. Un sistema que contiene información o datos fluidos y siempre cambiantes no contiene realmente documentos de archivo hasta que alguien decide realizarlos y guardarlos con *forma fija*[8] y *contenido estable*.[9]

[8] Definida como la cualidad de un documento de archivo que asegura que la apariencia o presentación documental es la misma cada vez que un documento de archivo es recuperado.
[9] Definido como la cualidad de un documento de archivo que convierte la información y los datos, contenidos en él, en inmutables; y requiere que se realicen cambios para añadir una actualización o crear un nueva versión.

Aunque la idea de contenido estable es bastante simple, el concepto de forma fija es más complejo. Esencialmente, significa que el mensaje comportado por un documento digital de archivo (u otro objeto digital), puede ser reproducido con la misma apariencia documental que tuvo en pantalla cuando fue realizado, recibido o guardado por primera vez. La secuencia de *bits* que componen el documento digital de archivo y determinan su presentación digital (por ejemplo, su formato de fichero), puede cambiar, pero su presentación documental no se debe modificar. Un ejemplo sencillo es cuando un documento creado en Microsoft Word se guarda posteriormente como un fichero Adobe PDF. Aunque la presentación digital del documento ha cambiado –de un formato de fichero .doc de Microsoft Word a un formato de fichero .PDF de Adobe–, la presentación gráfica del documento –también llamada su *forma documental*–[10] no ha cambiado, y por tanto podemos decir que el documento tiene forma fija.

En algunos casos, los materiales digitales pueden presentarse de maneras distintas. En otras palabras, la información que contienen puede adoptar diferentes formas documentales. Por ejemplo, los datos estadísticos pueden presentarse como un gráfico circular, un gráfico de barras o una tabla. Sin embargo, las posibles variaciones de estas visualizaciones están limitadas usualmente por el sistema. En tales casos, podemos considerar que cada presentación documental tiene contenido estable y forma fija, dado que la información se selecciona de un almacén fijo de datos dentro del sistema y las reglas del sistema regulan la forma de su(s) presentación(es) documental(es).

Una situación similar tiene lugar cuando la selección tanto del contenido como de la forma procede de un gran almacén de

[10] Definida como las reglas de representación de acuerdo con las cuales se comunican el contenido de un documento de archivo, su contexto administrativo y documental; y su autoridad. La forma documental posee elementos tanto extrínsecos como intrínsecos.

información fija a la que sólo se accede parcialmente cada vez que un usuario hace una petición al sistema. Si la misma petición siempre produce el mismo resultado en cuanto al contenido y a la forma documental, puede considerarse que el resultado tiene contenido estable y forma fija. De esta manera, como autor del documento de archivo, establece reglas fijas para la selección de su contenido y de su forma documental que sólo permitan una gama de variabilidad conocida y estable –esto es, los dotan con *variabilidad limitada*–,[11] entonces puede reivindicar que su material tiene contenido estable y forma fija.

El interés por la presentación documental de los materiales digitales es particularmente importante para mantener y ponderar la fiabilidad y exactitud de los documentos de archivo. Futuras actualizaciones, conversiones o migraciones de los datos pueden dar como resultado cambios en la forma documental. Por tanto, sería prudente establecer primero la forma documental de los documentos de archivo asociados con cada actividad o procedimiento y luego identificar las características esenciales (por ejemplo, los elementos esenciales intrínsecos y extrínsecos)[12] de cada presentación o forma documental. Esto le ayudará a alertarle de cualquier cambio en el futuro que pudiera implicar una pérdida de identidad y de integridad del documento de archivo, especialmente si se es activo en la esfera del arte digital, donde una descripción certificada por el artista

[11] Definida como la cualidad de un documento de archivo que asegura que sus presentaciones documentales están limitadas y controladas por reglas fijas y un almacén estable de datos de contenido, datos de forma y datos de composición, para que la misma actividad, petición, solicitud o interacción del usuario genere siempre el mismo resultado.

[12] *Elementos intrínsecos* se definen como los elementos de un documento de archivo que comportan la acción en la que participa y su contexto inmediato, incluidos los nombres de las personas implicadas en su creación, el nombre y la descripción de la acción o el asunto al que pertenece, la(s) fecha(s) de creación y transmisión; y demás. *Elementos extrínsecos* se definen como los elementos de un documento de archivo que constituyen su apariencia externa, incluidas las características de presentación como fuentes, gráficos, imágenes, sonidos, visualizaciones, hipervínculos, resoluciones de imagen y varios, así como firmas digitales, sellos y sellos de tiempo y signos especiales (marcas de agua digitales, logos, membretes, y demás).

de aquellas características esenciales ayudaría a dar soporte al reconocimiento de los derechos de propiedad intelectual vinculados a la obra así descrita.

3. Asegúrese de que los materiales digitales se identifican adecuadamente

Dar un nombre significativo a un fichero de ordenador ayuda a identificar su contenido y facilita encontrarlo. Sin embargo, la completa identificación de los documentos de archivo es más compleja que simplemente nombrar ficheros. La identificación completa es esencial para distinguir los documentos de archivo unos de otros, para distinguir diferentes versiones de un solo documento de archivo y para proporcionar evidencia de la identidad de un documento de archivo desde el momento de su creación hasta su preservación a largo plazo.[13]

A la información acerca de los materiales digitales que da soporte a su identificación y recuperación se hace referencia comúnmente como *metadatos*.[14] La mayoría de aplicaciones de *software* etiquetan automáticamente todos los materiales digitales con algunos datos acerca de su identidad, porque esta información es necesaria para localizar los documentos eficazmente. Sin metadatos, sería casi imposible encontrar un documento sin abrir y leer toda una carpeta o varios directorios. Los metadatos describen las propiedades o los atributos de los materiales digitales. En el caso de los documentos de archivo, sin embargo, estas propiedades o estos atributos también son necesarios para mantener y ponderar su autenticidad. Es por

[13] En este contexto, *identidad* se define como el total de las características de un documento o de un documento de archivo que lo identifican de manera única y lo distinguen de cualquier otro documento o documento de archivo. Con la integridad, representa un componente de la autenticidad.
[14] Definidos como información que caracteriza otro recurso de información, especialmente a efectos de documentar, describir, preservar o gestionar ese recurso.

ello que resulta primordial asegurar que todos los que se determinan esenciales se registren y sean correctos.

A las propiedades o los atributos que comportan la identidad de los materiales digitales se hace referencia como *metadatos* de identidad.[15] Éstos incluyen:

- Los nombres de las personas implicadas en la creación de los materiales digitales. Conformados por:
  - El autor. La (s) persona(s) física(s) o corporativa(s) responsable(s) de publicar los materiales.
  - El redactor. La(s) persona(s) física(s) o el(los) puesto(s) responsable(s) de articular el contenido de los materiales.
  - El generador. La persona física, el puesto o la oficina responsable de la cuenta electrónica o del entorno técnico donde los materiales se generan y desde el cual se transmiten.[16]
  - El destinatario. La(s) persona(s) física(s) o corporativa(s) para quien(es) está(n) destinado(s) los materiales.
  - El receptor. La(s) persona(s) física(s) o corporativa(s) para quien(es) los materiales pueden ser copiados o se le(s) puede enviar una copia ciega.
- *Nombre de la acción o tema*. En otras palabras, el título o el asunto.

[15] Definidos como las propiedades o atributos que comportan la identidad de un objeto digital que tiene que mantenerse como documento de archivo (véase, además, la Recomendación 5).
[16] La identificación del generador sólo es importante en los casos en que la persona, el puesto o la oficina responsables de crear y/o transmitir físicamente los materiales no es ni el autor ni el redactor; y cuando la presencia del nombre del generador que aparece en, o en asociación con, los materiales pone en cuestión al autor y/o redactor real de los materiales. Esto está asociado de la manera más común con correos electrónicos en casos en que el nombre del generador aparece en la cabecera de un correo electrónico y/o sus adjuntos que fueron de hecho creados y/o redactados por otra persona, pero físicamente manifestados y/o transmitidos en nombre de esa persona por el generador.

- Forma documental. Es decir, si es un informe, una carta, un contrato, una tabla, una lista y más.
- Presentación digital. Esto es, formato, contenedor o codificación, entre otros.
- Fecha(s) de creación y transmisión. Éstas incluyen:
    - La f*echa cronológica* escrita sobre los materiales, o en la cual éstos fueron compilados.
    - Las *fechas de transmisión y recepción*.
    - La *fecha archivística o de archivado* –en otras palabras, la fecha en que los materiales fueron asociados con una carpeta, un directorio informático o con otro cuadro de clasificación o plan de archivado (véase Recomendación 5).
- *Expresión del contexto documental* –por ejemplo, un código de clasificación, o el nombre de la carpeta o del directorio, o unidad de archivado comparable dentro del cuadro de clasificación o plan de archivo al que los materiales están asociados. Y el nombre del grupo más general de documentos de archivo al que los materiales pertenecen (véase además Recomendación 5).
    - Indicación de adjuntos, si es aplicable.
    - Indicación del copyright u otros derechos de propiedad intelectual, si es aplicable.
    - Indicación de la presencia o retirada de una firma digital, si es aplicable (véase Recomendación 6, sección de Autenticación Dependiente de la Tecnología).
    - Indicación de otras formas de autenticación, si es aplicable. Esto podría incluir, por ejemplo, la presencia de una corroboración (por ejemplo, una mención explícita de los medios utilizados para validar el documento de archivo); un testimonio (por ejemplo, la validación de un documento de archivo por aquellos que tomaron

parte en su publicación y por los testigos de la acción o la 'firma' del documento de archivo); una suscripción (por ejemplo, el nombre del autor o del redactor que aparece en la parte inferior del documento), o una cualificación de la firma (por ejemplo, la mención del título, de la capacidad y de la dirección de la persona o las personas que firman el documento de archivo).

- Indicación del número de borrador o versión, si es aplicable.
- Existencia y localización de materiales duplicados fuera del sistema digital, si es aplicable. Si existen múltiples copias de un documento, se debería indicar cuál es la copia oficial o autorizada.[17] Si el documento está certificado por el autor como una "reproducción aprobada" de una obra (por ejemplo, una obra de arte digital), se requiere la indicación de la existencia de tal certificación. Si el documento comprende material con copyright de diferentes autores, es necesaria la indicación de la acreditación de copyright (o de la falta del mismo) con las fechas relacionadas.

4. Asegúrese de que los materiales digitales contienen información que ayudará a verificar su integridad

Aunque los metadatos de identidad ayudan a distinguir unos materiales digitales de los demás, otro conjunto de metadatos permitirá a los usuarios inferir que los materiales son los mismos que cuando se crearon (aunque no lo verifican ni lo demuestran,

[17] Definida como la instancia de un documento de archivo que es considerado por el creador como el documento de archivo oficial y está usualmente sujeta a controles procedimentales que no se requieren para otras instancias.

porque esto requeriría la comparación con una copia de los materiales mantenidos en otro lugar). A estos metadatos puede hacerse referencia como *metadatos de integridad* (véase más abajo). Los materiales digitales tienen *integridad*[18] si están intactos e incorruptos, esto es, si los mensajes de los que se entiende que comunican para lograr sus propósitos están inalterados. Esto significa que la integridad física de los materiales digitales y el número adecuado de secuencias de *bits*, puede quedar comprometida, aun en el supuesto de que la articulación del contenido y los elementos requeridos de la *forma documental* (véase la Recomendación 2) sigan siendo los mismos. Se considera que el contenido y los datos dentro de él están inalterados si son idénticos, en cuanto a valor y presentación (por ejemplo, posición en pantalla), al contenido y a los datos que se guardaron en la primera manifestación del material. Los atributos que se refieren a la integridad de los materiales digitales tienen que ver con el mantenimiento de los materiales, incluida la responsabilidad de su adecuado tratamiento, como supervisar y documentar cualquier transformación tecnológica o transferencia de los materiales a otros sistemas.

Los metadatos de integridad incluyen:

- Nombres de la persona u oficina que trata los materiales. Puede ser la persona u oficina que usa los materiales para llevar a cabo negocios.
- Nombre de la persona u oficina con la responsabilidad primaria de mantener los materiales. Puede ser la misma que la de la persona u oficina de tratamiento.
- Indicación de las anotaciones añadidas a los materiales, si es aplicable.

[18] Definida como la cualidad de ser completo e inalterado en todos sus aspectos esenciales. Junto con identidad, un componente de autenticidad.

- Indicación de cualquier cambio técnico a los materiales o a la(s) aplicación(es) responsable(s) de gestionar y proporcionar acceso a los materiales por ejemplo, cambio de la codificación, contenedor o formato, actualización de una versión a otra de una aplicación, conversión de varios componentes digitales vinculados a un solo componente (por ejemplo, embebiendo directamente en los materiales componentes digitales que anteriormente sólo estaban vinculados a los materiales, como audio, video, gráfico o elementos de texto como fuentes).
- Código de restricción de acceso. Indicación de la persona, el puesto o la oficina autorizados a leer los materiales, si es aplicable.
- Código de privilegios de acceso. Indicación de la persona, el puesto o la oficina autorizados a anotar los materiales, borrarlos o retirarlos del sistema, si es aplicable.
- Código de documento de archivo vital. Indicación del grado de importancia del documento de archivo para continuar la actividad para la que fue creado o el negocio de la persona u oficina que lo creó, si es aplicable.[19]
- *Disposición planificada*. Por ejemplo, retirada del sistema vivo a un almacenamiento fuera del sistema; transferencia al cuidado de un custodio fiable (véase Recomendación 10); borrado programado.

5. Organice los materiales digitales en agrupamientos lógicos

La gestión y la recuperación de sus materiales digitales puede mejorarse si puede tratarlos en conjuntos grandes, más que

[19] El código de documento de archivo vital pertenece a comunidades específicas de práctica, como oficinas legales y médicas, que deben identificar los documentos de archivo que son vitales para la continuidad de su negocio en caso de desastre, y que por tanto ejercerían medidas especiales de protección sobre esos documentos de archivo.

de uno en uno. Por tanto, es importante que agrupe sus materiales digitales de alguna manera lógica. Las categorías elegidas pueden reflejar el modo en que se trabaja, sus actividades, procedimientos, áreas temáticas o algún tipo de organización estructural. Separar sus documentos de archivo de otros materiales digitales es un primer paso importante. La organización de sus documentos de archivo puede basarse en los diferentes tipos de documentos de archivo o en el periodo de tiempo durante el cual ciertos tipos de documentos de archivo tienen que mantenerse. Estos agrupamientos pueden estar relacionados unos con otros de manera jerárquica o plana, como mejor se adecue a sus necesidades. Generalmente, esta estructura debería ser coherente con la organización de cualquier documento de archivo en papel que tenga (o documentos de archivo en otros soportes), para que todos los documentos de archivo relacionados con la misma actividad o el mismo asunto, o del mismo tipo, puedan identificarse y recuperarse fácilmente como parte de un agrupamiento conceptual, a medida que se necesite. El cuadro de su organización debería registrarse en un documento que muestre todos los agrupamientos de los materiales, los describa con una frase breve e indique el modo en que se relacionan. En este documento, que se llama *Cuadro de clasificación*[20] o *Plan de archivado*, a cada agrupamiento de documentos de archivo se le puede asignar un código o un nombre que debería vincularse a cada documento de archivo que pertenezca al mismo agrupamiento, no importa en qué soporte o localización: así, los documentos de archivo asignados a cada agrupamiento compartirán tal código o nombre, seguido por un número que indica su secuencia. Este identificador debería registrarse entre los metadatos de identidad[21] de sus

[20] Definido como un plan para la identificación y la organización sistemáticas de las actividades de negocio y los documentos de archivo en categorías de acuerdo con convenciones, métodos y reglas de procedimiento estructuradas lógicamente (véase, además, la Recomendación 3).
[21] Definidos como las propiedades o atributos que comportan la identidad de un objeto digital que tiene que mantenerse como documento de archivo (véase, además, la Recomendación 3).

documentos digitales de archivo y en la superficie de sus documentos de archivo en papel que pertenecen al mismo agrupamiento, y deberían ser únicos para cada documento de archivo.

Identificar durante cuánto tiempo los agrupamientos de documentos de archivo tendrán que retenerse facilitará su gestión mientras se necesiten regularmente y ayudará a asegurar que los documentos de archivo que necesitan o merecen preservación a largo plazo se etiquetan prontamente y se les proporciona una protección adecuada para asegurar su supervivencia.

Se encontrará más fácil y más eficaz asignar un periodo de retención –el tiempo durante el que quiere o tiene que mantener los materiales–, a una agrupación de materiales, más que a ítems individuales. Asegurar que algunas cosas se mantengan durante tanto tiempo como se necesite, mientras que se expurguen cosas que ya no son necesarias es, simplemente, demasiado pesado a nivel de ítem individual. Aunque puede que se piense que dentro de un agrupamiento algunos documentos de archivo deberían mantenerse más tiempo que otros, no sólo ahorrará tiempo si mantiene todo el agrupamiento, sino que también tendrá información más completa cuando necesite hacer referencia a los documentos de archivo. Sin embargo, para algunos tipos de documentos de archivo, puede crear subgrupos dentro de cada agrupamiento, dado sobre la base del periodo de retención.

6. Utilice técnicas de autenticación que promuevan el mantenimiento y la preservación de los materiales digitales

La autenticidad de los materiales digitales está amenazada siempre que se transmite desplazándose en el espacio (por ejemplo, cuando se envía a un destinatario o entre sistema o aplicaciones), en el tiempo (por ejemplo, cuando están en almacenamiento, o cuando el *hardware* o el *software* utilizado para

almacenarlos, procesarlos o comunicarlos se actualizan o se reemplazan). Puesto que los actos de guardar materiales para acción o referencia futuras, o recuperarlos, inevitablemente implican moverlos entre significativas fronteras tecnológicas (desde el subsistema de visualización al de almacenamiento y viceversa), la inferencia de la autenticidad de los materiales digitales debe venir apoyada adicionalmente por evidencia de que han sido mantenidos utilizando tecnologías y procedimientos administrativos que garantizan su identidad e integridad continuadas, o al menos minimizan los riesgos de cambio desde el momento en que los documentos de archivo fueron guardados por primera vez hasta el punto en el que se accede a ellos posteriormente.

Autenticación independiente de la tecnología

Presunción de autenticidad. Es una inferencia que se extrae de hechos conocidos acerca de la manera en que un documento ha sido creado y mantenido. La adopción y la aplicación coherente de las recomendaciones presentadas en este documento proporcionan la mejor evidencia en apoyo de tal presunción. Las recomendaciones son acumulativas: a mayor número de recomendaciones satisfechas y a mayor grado en que una recomendación individual se satisface, más fuerte es la presunción de autenticidad.

La implantación con éxito de las recomendaciones presentadas en este documento se predica sobre el establecimiento y la aplicación continua de políticas y procedimientos administrativos eficaces.[22] Idealmente, debería esforzarse por implantar técnicas de autenticación apoyadas por políticas y procedimientos administrativos que sean tan independientes y neutrales, con respecto a la tecnología, como sea posible.

[22] Véase Apéndice 19, "A Framework of Principles for the Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records".

Autenticación dependiente de la tecnología

Las técnicas de autenticación dependientes de la tecnología, como la criptografía, se utilizan para proporcionar un mecanismo tecnológico para garantizar la autenticidad de los materiales digitales. Una de tales técnicas criptográficas es la firma digital, que puede utilizarse cuando se transmiten documentos entre personas, sistemas o aplicaciones para declarar su autenticidad en un cierto punto del tiempo. A tales tecnologías les ha sido dado valor legal o regulatorio por algunos cuerpos, como la Comisión Europea y la Securities and Exchange Commission.

¡Precaución! Las firmas digitales están sujetas a obsolescencia, en virtud de su propósito y de su funcionalidad inherente, no pueden migrarse a aplicaciones de *software* nuevas o actualizadas junto con los documentos a las que están adjuntas. De hecho, puede que la vida de las firmas digitales y otras tecnologías de autenticación sea mucho más corta que el periodo de tiempo durante el que incluso un documento temporal que no requiere migración puede que tenga que ser mantenido, porque la tecnología de autenticación está cambiando rápidamente. A menos que, o hasta que, posteriores desarrollos de la tecnología de firma digital hagan posible que tal información encriptada sobre autenticación se pueda preservar a lo largo del tiempo con el documento. Se debería, cuando recibe un documento con una firma digital adjunta, separar la firma siempre que sea posible y añadir información a los metadatos de integridad, para indicar que el documento tuvo una firma digital adjunta cuando se recibió, y que la firma fue verificada, separada y borrada.

7. Proteja los materiales digitales de acciones no autorizadas

La exactitud y la autenticidad de los materiales digitales no puede presumirse si existe alguna oportunidad de modificarlos

sin dejar rastro. Por ello, se tiene que ser capaz de demostrar que fue imposible para cualquiera alterar o manipular sus materiales digitales sin que esa persona estuviera identificada. La seguridad incluye restringir el acceso físico a los lugares donde se mantienen las computadoras personales, así como restringir el acceso a los materiales digitales que se encuentran en éstos, lo cual puede lograrse mediante varios medios, incluidos el uso de contraseñas o autenticación biométrica para entrar en el sistema.

También es importante establecer una estructura de permisos de acceso (también llamados privilegios de acceso –véase la discusión sobre los metadatos de integridad en la Recomendación 4–), para todos los usuarios del sistema. Por ejemplo, puede que algunos sólo sean capaces de leer los materiales, mientras que otros tengan permiso para modificarlos. En cualquier caso, debería ser imposible modificar cualquier documento de archivo una vez que se ha archivado, de acuerdo con el cuadro de clasificación o el plan de archivado (véanse Recomendaciones 3 y 5); y sólo la persona a quien se ha asignado la responsabilidad sobre la gestión y el mantenimiento de los documentos de archivo debería ser capaz de transferir o borrar materiales del sistema. Además, el sistema debería mantener una pista de auditoría para rastrear el acceso a los materiales, para controlar la administración y el uso de los privilegios de acceso.

Puede que esta recomendación parezca demasiado pedir para individuos que trabajan desde sus casas. Incluso para los que trabajan en oficinas o en comunidades de práctica muy pequeñas. Sin embargo, es esencial recordar que si no puede demostrar que fue imposible para cualquiera alterar y manipular sus materiales digitales sin ser identificado, su confirmación de que sus documentos de archivo son de facto exactos y auténticos resulta irrelevante. A este respecto, podría resultar útil mantener copias de al menos los materiales digitales más importantes

fuera de línea y establecer alguna rutina mediante la cual los materiales almacenados fuera de línea se comparen aleatoriamente con sus contrapartidas en línea de manera periódica.

8. Proteja los materiales digitales de pérdida y corrupción accidentales

Las computadoras no son infalibles y un cierto número de factores pueden causar corrupción u otra pérdida accidental de documentos de archivo o datos. La mejor manera de asegurarse contra pérdida o corrupción accidentales es realizar copias de seguridad de manera regular y a menudo. Si las almacena fuera de línea, se obtiene una protección adicional contra el fuego o el robo de equipamiento. Existen muchas técnicas de copia de seguridad, paquetes de *software* y servicios, incluidos aquellos que automáticamente crean los materiales de copia de seguridad y luego los transmiten a una localización segura fuera de línea.

- *Desarrolle una política o rutina rigurosa que asegure que se hace copia de seguridad diaria de su sistema.* Su sistema sólo es tan bueno como su última copia de seguridad, de modo que tiene que estar confiado en que se hace copia de seguridad a menudo, al menos una vez al día, utilizando métodos probados que aseguren que si algo va mal, el usuario y su negocio serán capaces de recuperarse rápidamente. Las copias de seguridad regulares deberían destruirse sobre una base rotacional, de acuerdo con una estrategia o un calendario que sean los más adecuados para sus requisitos, dado que no contienen documentos de archivo, sino que sólo existen para la recuperación del sistema si falla. Aquí estamos hablando acerca de una *copia de seguridad del sistema* comprehensiva, que incluye

el sistema operativo, las aplicaciones de *software* y todos los materiales digitales dentro de su sistema. Si además de una copia de seguridad del sistema se necesita una copia de seguridad de sus materiales digitales en el caso de que su computadora sea robada o algunos de sus documentos de archivo devengan corruptos, entonces se debería hacer copia de seguridad de esos materiales sólo en otra computadora, en un disco duro externo o en otros soportes digitales portátiles y almacenar estas copias de seguridad en una localización fuera de línea y lejos de la computadora con las copias "originales".

- *Elija e instale la mejor tecnología de copia de seguridad para su situación*. Estudie la tecnología y los servicios disponibles; y seleccione aquellos que mejor funcionen para su situación particular. Existen muchos sistemas diferentes, que abarcan desde los que cubren las operaciones de una persona hasta aquellos capaces de hacer copias de seguridad de sistemas muy grandes. El sistema de copia de seguridad tiene que incluir una pista de auditoría, en el caso de que el sistema falle entre copias de seguridad y se tengan que recuperar los documentos de archivo u otros materiales digitales creados durante el tiempo para el que no hay copia de seguridad.

9. Adopte medidas contra la obsolescencia del hardware y del software

La velocidad con la que el *hardware* y el *software* se vuelven obsoletos, plantea severos retos al mantenimiento y la preservación a largo plazo del material digital. Una estrategia para abordar este problema es eliminar la dependencia del *hardware* transfiriendo las funcionalidades del *hardware* al *software* (por ejemplo, utilizar una aplicación de software para simular

las acciones de una pieza de hardware). Esto proporciona una manera más estable de retener la función cuando el *hardware* se hace vetusto.

El entorno tecnológico cambiante significa que tanto los individuos como las oficinas deberían actualizar regularmente sus sistemas digitales, así como los documentos de archivo dentro de estos sistemas y aquellos que han sido trasladados a otros soportes de almacenamiento, como CD, DVD o cinta. En otras palabras, cuando las partes del entorno tecnológico en el que se está trabajando comienzan a hacerse viejos, deberían actualizarse a la más avanzada tecnología disponible de acuerdo con sus requisitos y restricciones particulares; y todos los materiales digitales, dentro y fuera del sistema, deberían migrar a la nueva tecnología. Cuando se reemplaza *hardware*, es importante para esta reposición el que el *hardware* tenga capacidades al menos iguales al que está reemplazando. Por ejemplo, un monitor nuevo tiene que visualizar un documento gráfico de archivo de manera que retenga la forma documental del documento de archivo original. La planificación de actualizaciones regulares de tecnología sobre una base rotacional le ayudará a asegurar que su tecnología no deviene caduca y también ayuda a evitar grandes e inesperados gastos tecnológicos.

A veces, los documentos digitales de archivo producidos por, o mantenidos en, sistemas que se están volviendo obsoletos tienen que retenerse durante largo tiempo, pero no se espera que se acceda a ellos a menudo. Si tales documentos de archivo son documentos textuales de archivo y tienen que leerse secuencialmente, más que aleatoriamente, podría convertirlos de su forma digital a microfilm con salida por computadora. Esto los protegerá de pérdida o corrupción accidentales mejor que cualquier otra medida. Otro buen recurso protector es la duplicación: crear una segunda copia de grupos de documentos vitales de archivo y mantenerla en otra computadora, en un segundo disco

duro, en DVD, con otra oficina u otro individuo; o en un almacenamiento remoto. Cuando los documentos digitales de archivo u otras entidades se retiran de un sistema vivo, por ejemplo, para su almacenamiento sobre soporte magnético u óptico fuera del sistema, es esencial que la documentación del sistema y de los materiales digitales (por ejemplo, los metadatos de los documentos de archivo) también se retire y se mantenga con ellos. Para información más detallada acerca de los tipos de documentación comentados, véase la Recomendación 1, subsecciones D, E y F.

10. Considere los problemas que circundan a la conservación a largo plazo

Aunque el enfoque de este documento se ha puesto en la creación y el mantenimiento de todos los tipos de materiales digitales, mientras se necesiten de manera regular por parte de sus creadores, es importante considerar el modo en que mejor se preservan materiales digitales importantes a largo plazo. De manera típica, sólo un pequeño porcentaje tiene que resguardarse a largo plazo, pero la capacidad para proporcionar cuidado permanente y a largo plazo a los materiales, especialmente a los digitales, está a menudo más allá de la capacidad o el interés de individuos y pequeños organismos. La retención de materiales a largo plazo implica costos reales –tanto financieros como humanos–, pero tales esfuerzos de preservación son esenciales para establecer y mantener nuestro patrimonio cultural, a efectos de responsabilidad; y para informar la toma de decisiones gerencial.

Para comenzar este proceso, se debe designar a alguien que se haga cargo de los materiales digitales, una vez que ya no se necesitan para los propósitos personales o profesionales. Esta persona designada adoptaría el papel de un custodio fiable.[23]

[23] Definido como un preservador que puede demostrar que no tiene motivo para alterar los documentos de archivo preservados o para permitir que otros los alteren, y que es capaz de implantar todos los requisitos para una preservación auténtica de los documentos de archivo.

Un custodio fiable es un profesional –o grupo de profesionales, como en un archivo o en una sociedad histórica–, que ha sido preparado en cuanto a gestión y preservación de documentos de archivo y que, idealmente, no tiene interés en el contenido de los documentos de archivo, ni por qué permitir que otros los manipulen o los destruyan.

En el caso de organizaciones u oficinas pequeñas, esta persona podría ser responsable de mantener, organizar y almacenar los documentos de archivo durante su uso activo. En el caso de individuos que negocian su propia gestión de documentos, la persona que satisface la función de preservación puede ser un archivero o un bibliotecario de un centro de documentación; o simplemente ellos mismos. En cualquier caso, debería establecerse una estrategia de preservación tan pronto como fuera posible, porque los materiales digitales que no han sido elegidos para preservación prontamente y que no han sido objeto de cuidado de manera proactiva, no serán preservados. La íntima adhesión a estas recomendaciones, por tanto, facilitará la preservación a largo plazo.

Conclusión

Este documento ha delineado una serie de actividades para que los individuos y las organizaciones pequeñas lleven a cabo la creación y el mantenimiento de materiales digitales de los que se puede presumir que son auténticos, exactos y fiables. Para los individuos la carga puede parecer grande, pero la alternativa –pérdida de documentos de archivo o la aparición de datos corruptos y no verificables– sería un problema mayor a la larga. Las pequeñas organizaciones se beneficiarán de la realización de una clara designación del o los individuos responsables de supervisar el mantenimiento de los documentos digitales de archivo de la organización. Sin embargo, se debe tener en cuenta que no todas las recomendaciones presentadas en este

documento tienen que implantarse en todas las circunstancias; hay que ser capaz de seleccionar y adoptar las medidas que abordan sus problemas particulares en el contexto específico en el que funciona. Puede que también existan casos en que sean necesarias medidas adicionales a causa de requisitos legislativos o reguladores específicos de su campo; o de las características de la actividad y, de ahí, de los documentos de archivo que produce. En tales casos, puede que se requiera la consulta con expertos. Entre tales expertos se encuentran los archiveros municipales, provinciales, estatales o nacionales, así como las asociaciones locales de archiveros. Los individuos, las oficinas y las organizaciones pequeñas no deberían dudar en contactar a tales expertos en busca de consejo sobre cualquier problema relacionado con la creación y el mantenimiento de sus materiales digitales.

Finalmente, este conjunto de recomendaciones no es sino uno de los documentos publicados por el Proyecto InterPARES, un proyecto internacional de investigación que estudia la preservación a largo plazo de documentos digitales de archivo auténticos. Material adicional, que da soporte a la comprensión de la naturaleza de los documentos digitales de archivo y del desarrollo de métodos para su creación fiable y su mantenimiento y su preservación exactos y auténticos, puede encontrarse en el sitio Web de InterPARES en www.Interpares.org.

Apéndice D: Recomendaciones para el preservador. Preservar documentos digitales de archivo: recomendaciones para las organizaciones[24]

Introducción

Estas recomendaciones han sido desarrolladas para proporcionar consejo concreto a diversos grupos que son responsables de la preservación a largo plazo de documentos digitales de archivo. No están orientadas a ser comprehensivas, sino a destacar un cierto número de áreas que son particularmente importantes para la preservación de documentos digitales de archivo auténticos; y sobre los cuales la experiencia ha mostrado que a menudo son pasadas por alto en la carrera por aceptar documentos digitales de archivo en depósitos archivísticos.

Se reconoce extensamente que los documentos digitales de archivo deben ser cuidadosamente gestionados a lo largo de toda su existencia para asegurar que son accesibles y legibles a lo largo del tiempo con su forma, contenido y relaciones intactos, en la medida necesaria para dotarles de carácter fidedigno continuado como documentos de archivo. También se acepta ampliamente que la gestión de documentos digitales de archivo debe proceder desde un entendimiento comprehensivo de todas las fases o etapas de la existencia de los documentos digitales de archivo, desde el momento en que se generan, durante su mantenimiento por parte de su creador y durante su valoración, disposición y preservación a largo plazo, como memoriales auténticos de las acciones y los asuntos de los que

[24] Estas recomendaciones también han sido publicadas en forma de folleto ilustrado, disponible de forma gratuita en http://www.interpares.org/display_file.cfm?doc=ip2(pub)preserver_guidelines_booklet.pdf. (Estas recomendaciones han sido incluidas directamente desde el sitio *Web* de InterPARES. Los apéndices a los que se hace referencia en estas Recomendaciones se refieren al libro IP2. Esto se aclarará y fijará cuando se apruebe el método de distribución y el contenido final).

son parte. Desde la perspectiva de la preservación a largo plazo, todas las actividades para gestionar documentos de archivo a lo largo de su existencia están vinculadas, como una cadena; y son interdependientes. Si un eslabón de la cadena falla, el resto no puede hacer su trabajo. Si no se emprenden ciertas actividades y acciones sobre los documentos de archivo, su integridad (esto es, su fiabilidad y su autenticidad), así como su preservación, están en peligro.

Estas recomendaciones se enfocan sobre los eslabones de preservación en la cadena y se organizan de acuerdo con la secuencia de actividades de preservación presentadas en el modelo Cadena de Preservación (COP) de InterPARES[25] que traza los pasos secuenciales en la creación, mantenimiento y preservación de documentos digitales auténticos. El número alfanumérico entre paréntesis que sigue al título de cada sección en estas Recomendaciones es una referencia cruzada a la actividad de preservación aplicable presentada en el modelo COP.

Las recomendaciones han sido adaptadas para abordar las necesidades de preservación de organizaciones o programas cuyos documentos de archivo deben retenerse y consultarse durante largos periodos y las de instituciones archivísticas que asumen la responsabilidad de preservación de los documentos de archivo de otros y de su accesibilidad continuada al público al que sirven. En ambos casos, los recursos humanos y financieros, así como la experiencia técnica interna, están frecuentemente limitados.

Las instituciones, las organizaciones y los programas con responsabilidades de preservación también deberían consultar el *Framework of Principles for the Development of Policies,*

[25] Disponible en http://www.interpares.org/ip2/ip2_models.cfm.

Strategies and Standards for the Long-term Preservation of Digital Records (también conocido como el Policy Framework)[26] desarrollado por el Dominio Cruzado de Política de InterPARES 2, que complementa a estas Recomendaciones. Muchas de las indicaciones de estas Recomendaciones pueden ser aplicables a la preservación de objetos digitales distintos de los documentos de archivo, como documentos, publicaciones o datos.

Gestionar la cadena de preservación

Este aspecto implica determinar los requisitos de la estructura de referencia y diseñar, implantar y mantener una *Cadena de Preservación Marco*, que incluye todos los elementos de política, estrategia, metodología, y varios más.

Establezca alcance y objetivos

Los preservadores deben definir el alcance y los objetivos de su programa de preservación digital. En las artes, por ejemplo, puede que deseen preservar la grabación de la(s) ejecución(es) de una obra, o puede que elijan emprender una preservación más compleja de los componentes de una obra de arte que dan soporte a su reproducción o re-ejecución. En las ciencias, puede que deseen preservar sólo el informe final de los resultados de un experimento o mantener los datos brutos, los datos normalizados o los datos agregados para documentar la metodología utilizada y el resultado obtenido, así como para asegurar la disponibilidad de los datos para usos futuros. Los preservadores también deberían considerar quiénes serán los usuarios finales de los archivos. Los usuarios técnicamente sofisticados generalmente requieren menos asistencia para acceder incluso a materiales digitales tecnológicamente complejos, mientras que el

[26] Disponible en http://www.interpares.org/public_documents/ip2(pub)policy_framework_document.pdf.

público general podría requerir mecanismos de acceso extremadamente amistosos con el usuario y materiales transformados en unos pocos formatos sencillos, pero extensamente disponibles. El alcance del programa de preservación ayudará a definir a qué estrategias de preservación (véase sección 4 y el Apéndice 21c, sección B), podría tener que dar soporte un preservador.

Para definir el programa de preservación digital, los preservadores deberían basarse en esfuerzos previos. Para desarrollar políticas y estrategias adecuadas, los preservadores deberían consultar el Marco de Política de InterPARES 2, como orientación aplicable a niveles organizacional, sectorial, nacional, internacional y supranacional. Para las funciones del programa de preservación, los preservadores deberían consultar la norma ISO *Open Archival Information System* (OAIS)[27] y seguir el modelo Cadena de Preservación de InterPARES 2 para una adaptación de la norma OAIS específicamente dirigida a los documentos digitales de archivo. Los planes también deberían reflejar los *Trustworthy Repositories Audit & Certification: Criteria and Checklist*, una versión revisada y expandida de la *Audit Checklist for Certifying Digital Repositories*, originalmente desarrollada por la NARA/RLG Digital Repository Task Force.[28]

Adquirir recursos

La preservación digital requiere sustanciales recursos en financiamiento, competencias tecnológicas y experiencia. Una organización responsable de la preservación digital tiene varias opciones, incluidas: a) adquirir nuevos recursos, b) reasignar recursos existentes y; c) aprovechar otros recursos.

[27] International Organization for Standardization, ISO 14721: 2003 –Space data and information transfer systems–. Open archival information system-Reference model.
[28] Véase Online Computer Library Center, Center for Research Libraries (2007), "Trustworthy Repositories Audit & Certification: Criteria and Checklist", v. 1.0, February 2007. Disponible en http://www.crl.edu/PDF/trac.pdf.

Con independencia de la(s) opción(es) elegida(s), un requisito fundamental es que los recursos deben ser sostenibles. Los recursos de una sola vez, como las subvenciones, pueden ser adecuadas para tareas finitas específicas, como establecer el programa de preservación o procesar un cuerpo dado de documentos de archivo, pero una fuente fiable de recursos sostenidos es una condición *sine qua non* para cualquier programa de preservación.

Adquirir nuevos recursos financieros requerirá un sólido esquema para el programa y un correspondiente plan de comunicaciones para convencer a las fuentes de financiación y a las partes interesadas a las que es probable que los preservadores consulten el programa que debería ser financiado. Una estrategia viable para un nuevo programa puede ser comenzar por poco y planificar éxitos a corto plazo para convencer a las fuentes de financiación de que crezcan de manera incremental los recursos para el programa. Una estrategia como ésta debería evaluar si es más probable que las fuentes de financiación estén influidas por el éxito a corto plazo en objetivos básicos del programa o en áreas de preocupación más particular para las fuentes de financiación y las partes interesadas. Por ejemplo, puede que los financistas y las partes interesadas estén más inclinados hacia demostraciones de capacidades tecnológicas que hacia un plan de valoración de documentos digitales de archivo sólido y comprehensivo.

Para la mayoría de las organizaciones, es probable que reasignar recursos para la preservación digital implique decisiones dolorosas. Como con la búsqueda de nuevos fondos, quizá sea mejor una aproximación incremental. Además, pueden hacerse ajustes permanentes al plan, basándose en la experiencia obtenida durante cada fase de la implantación. Si el programa tiene que establecerse en una institución más grande, sería de ayuda abordar la preservación digital como parte del plan estratégico general, más que como una iniciativa especial.

Incluso, cuando un preservador adquiere con éxito nuevos recursos, o es capaz de reasignar los recursos existentes a la preservación digital, es improbable que tenga medios suficientes para abordar todos los retos. Por tanto, los preservadores deberían capitalizar las oportunidades de aprovechar recursos externos. Existen diversas maneras de hacer esto. Por ejemplo, más que tratar de contratar expertos técnicos sobre una base permanente o personal de formación en todos los conocimientos y habilidades técnicas requeridas, los preservadores podrían contratar expertos externos sobre la base de una consultoría o una tarea. No deberían excluir opciones para contratar tanto servicios básicos como *ad hoc*. A un nivel básico, los preservadores deberían evaluar la posibilidad de utilizar a un proveedor de servicios informáticos, más que adquirir un sistema de preservación dedicado. Las opciones *ad hoc* incluyen contratar compañías especializadas para tareas como re-copiar a partir de soportes digitales obsoletos o convertir formatos raros. Otra opción es participar –de manera activa o pasiva– en comunidades de fuente abierta que desarrollan las tecnologías necesarias para la preservación digital (por ejemplo, FEDORA,[29] Global Registry of Digital Formats).[30]

Finalmente, los preservadores de una organización a la que le faltan los recursos requeridos para dar soporte a un programa de preservación digital deberían investigar la posibilidad de establecer sociedades o consorcios cooperativos para desarrollar y financiar un programa que satisfaga una norma mínima aceptable.

Enfoque sobre los documentos digitales de archivo

Los preservadores deben asegurar que los recursos de preservación digital se despliegan primariamente para proteger las

[29] Véase http://www.fedora.info/
[30] Véase http://hul.harvard.edu/formatregistry/

copias autorizadas[31] de documentos digitales de archivo, más que para preservar copias digitalizadas de documentos analógicos de archivo que han sobrevivido. El fundamento para esto es que la mayoría de los documentos analógicos de archivo sobrevivirán sin digitalización, mientras que los documentos digitales de archivo se perderán sin un programa de preservación digital.

Ofrecer consejo

Puesto que la cadena de preservación de los documentos digitales de archivo comienza con la creación, los preservadores deberían proporcionar consejo sobre la creación y el mantenimiento de documentos digitales de archivo. Dependiendo del mandato del preservador, esto puede estar orientado de manera bastante específica a, por ejemplo, los empleados de la organización del preservador o, como en el caso de archivos nacionales, a otras instituciones gubernamentales. En otros casos, este consejo puede diseminarse de manera extensa a grupos de especial interés o al público general, con el propósito de llegar hasta la(s) persona(s) u organización(es) cuyos documentos de archivo caen bajo el mandato del preservador.

Establecer un buen ejemplo

Los preservadores deben establecer, en su organización, un entorno de creación y gestión de documentos tal, que sus propios documentos de archivo de control producidos en el curso de su función de preservación sean creados y mantenidos de manera que satisfagan los Requisitos de Cota que Apoyan

[31] Copia autorizada se define como "La representación de un documento de archivo que es considerada por el creador como el documento de archivo oficial y que está sujeta usualmente a controles procedimentales que no se requieren para otras representaciones" (InterPARES 2 Terminology Database. Disponible en http://www.interpares.org/ip2/ip2_terminology_db.cfm).

la Presunción de Autenticidad de Documentos Electrónicos de Archivo de InterPARES 1.[32] Esto no es sólo un requisito esencial para cualquier organización que emprenda preservación a largo plazo, sino que el desarrollo de este tipo de entorno interno también proporcionará:

- Formación práctica para los archiveros en las tecnologías que están defendiendo ante los creadores de documentos de archivo.
- Una inestimable "visión desde el punto de vista del usuario" de las soluciones reales de gestión de documentos y del modo en que realmente funcionan en un entorno operativo cotidiano.
- Un banco de prueba en el que pueden introducirse y evaluarse innovaciones.
- Un prototipo de trabajo que puede utilizarse en demostraciones.

Desarrollar procedimientos

Los preservadores deben establecer controles sobre la transferencia, el mantenimiento y la reproducción de documentos de archivo, incluidos los procedimientos y sistema(s) utilizados para transferir documentos de archivo a su propia organización o programa dentro de la organización; mantenerlos y reproducirlos de manera que satisfagan los Requisitos de Base que Apoyan la Producción de Copias Auténticas de Documentos Electrónicos de Archivo de InterPARES 1.[33] Estos procedimientos

[32] Véase Authenticity Task Force (2002), "Appendix 2: Requirements for Assessing and Maintaining the Authenticity of Electronic Records," en The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project, Luciana Duranti, ed. (San Miniato, Italy: Archilab, 2005), pp. 204-219. Reimpresión en línea disponible en http://www.interpares.org/book/interpares_book_k_app02.pdf. Véase el Apéndice 21a para una versión abreviada.

[33] *Ibid.* Véase Apéndice 21b para una versión abreviada.

deben incorporar controles adecuados y eficaces para garantizar la identidad[34] y la integridad[35] de los documentos de archivo, y específicamente que:

- Se mantiene sin rupturas la custodia de los documentos de archivo.
- Se implantan y supervisan procedimientos de seguridad y control.
- El contenido de los documentos de archivo y las anotaciones y elementos requeridos de la forma documental permanecen sin cambios después de la reproducción.

Implantar estrategias de mantenimiento

Aunque se presta mucha atención al desarrollo de complejas estrategias de preservación a largo plazo, son inaplicables si los documentos de archivo para los que van a ser utilizadas no se mantienen y protegen adecuadamente en el sistema de gestión de documentos y/o el sistema de preservación de documentos de archivo que los contienen. Una versión completa de las ocho estrategias primarias de mantenimiento se encuentra en el Apéndice 21c, sección A. Brevemente, incluyen:

A1. Una clara asignación de responsabilidades.
A2. Provisión de una infraestructura técnica adecuada.
A3. Implantación de un plan de mantenimiento, soporte y sustitución del sistema.

[34] *Identidad* se define como "El total de características de un documento o un documento de archivo que lo identifican de manera única y lo distinguen de cualquier otro documento o documento de archivo. Junto con la integridad, un componente de la autenticidad" (InterPARES 2 *Terminology Database*, *op. cit.*).
[35] *Integridad* se define como "La cualidad de ser completo e inalterado en todos los componentes esenciales. Junto con la identidad, un componente de la autenticidad" (*ibid.*).

A4. Implantación de un plan para la transferencia de documentos de archivo a un nuevo soporte de almacenamiento de manera regular.
A5. Adhesión a las condiciones de almacenamiento y tratamiento adecuadas para los soportes de almacenamiento.
A6. Redundancia y copia regular de seguridad de los objetos digitales.
A7. Establecimiento de un sistema de seguridad.
A8. Planificación de desastres.

Valorar los documentos de archivo para su conservación permanente (A4.2)

En los casos en que, como se recomienda en el modelo Cadena de Preservación de InterPARES 2, se emplee un calendario de retención, se tomarán decisiones sobre la disposición de los documentos de archivo de manera regular como parte de un sistema de gestión de documentos. En algunos casos, las valoraciones pueden ejecutarse cuando se determina que los documentos de archivo de un sistema existente desde hace mucho tiempo tienen que llegar a una disposición. Más abajo se discuten ocho aspectos importantes del proceso de valoración.

Evaluar de manera temprana

Dadas las dificultades técnicas implicadas en la preservación de documentos digitales de archivo, la identificación de qué documentos de archivo deben preservarse a largo plazo, debería llevarse a cabo en la oportunidad más temprana posible. La ejecución de la valoración, estableciendo métodos de transferencia e incluso identificando potenciales estrategias de preservación con el creador de los documentos de archivo, mejorarán la probabilidad de éxito. Este proceso también puede proporcionar al preservador una oportunidad para ofrecer consejo

sobre la creación y el mantenimiento de documentos de archivo (véase sección 1.4).

A los preservadores profesionales, como a los archiveros, se les anima frecuentemente a participar en el diseño de las aplicaciones informáticas que están siendo desarrolladas por las organizaciones con las que tienen una relación de donante-conservador. Esta aproximación ayudará a integrar prácticas adecuadas de gestión de documentos y preservación. Los preservadores que se han unido a equipos de diseño de sistemas han aprendido que es una práctica que consume una cantidad enorme de tiempo y que requiere una comprensión mucho más detallada de los flujos de trabajo y procedimientos de la organización, que la que un archivero adquiere normalmente durante una valoración. Además, las especificaciones del sistema raramente son una representación de la aplicación que finalmente será implantada. Aún tendrá que ejecutarse una valoración una vez que el sistema esté activo, satisfaciendo los requisitos organizacionales. Puede que sea más razonable para los archiveros contribuir al diseño del sistema como parte de la función de consejo discutida en la sección 1.4. Puede que se pruebe que compartir estrategias, principios y recomendaciones de alto nivel desarrollados por la profesión archivística sea un fin más real.[36]

Localizar a múltiples propietarios

En los casos en los que los componentes intelectuales de un objeto digital tienen múltiples propietarios, éstos deben

[36] En años recientes se han estudiado muchos aspectos relativos a la creación de programas de preservación eficaces. Entre los sitios web que contienen información o ejemplos útiles están: el Proyecto InterPARES en http://www.interpares.org; Model Requirements for the Management of Electronic Records (MoReq) en http://www.cornwell.co.uk/edrm/moreq.asp; Metadata Encoding and Transmission Standard (METS) en http://www.loc.gov/standards/mets/; Electronic Records from Office Systems (EROS) del Archivo Nacional del Reino Unido en http://www.nationalarchives.gov.uk/electronicrecords/advice/guidelines.htm; y el manual australiano DIRKS (Designing and Implementing Recordkeeping Systems) en http://www.records.nsw.gov.au/recordkeeping/dirks-manual_4226.asp.

identificarse durante el proceso de valoración para ponderar las ramificaciones de esta situación para la preservación a largo plazo. Esto puede suceder, por ejemplo, si las instituciones a diversos niveles del gobierno contribuyen y comparten acceso a recursos de datos. Otro ejemplo viene ilustrado por los sitios Web que acceden a, y utilizan recursos de información localizados fuera de su espacio de control. Aunque en estas circunstancias frecuentemente se negocian acuerdos de acceso, raramente incluyen provisiones para la preservación a largo plazo de todos los componentes digitales significativos.

Ponderar la autenticidad

Esto siempre ha formado parte del proceso tradicional de valoración archivística. En primera instancia, se ha fiado en la confirmación de la existencia de una cadena sin rupturas de custodia, desde el momento de la creación de los documentos de archivo hasta su transferencia a la entidad archivística responsable de su preservación a largo plazo. Los periodos en que los documentos de archivo no están sujetos a alguna forma de medidas protectoras por parte del creador de los documentos de archivo o por la institución sucesora con un interés establecido en mantener la exactitud y la completitud de los documentos de archivo, pueden arrojar dudas significativas sobre la autenticidad de los documentos de archivo.

La ponderación de la autenticidad también ha dependido del conocimiento del archivero de las prácticas de gestión de documentos, tanto históricamente como en relación con los tipos de documentos de archivo y los procedimientos administrativos de un creador específico. El marco general para esta ponderación fue codificada originalmente por la diplomática.[37] Un tercer

[37] Véase la discusión de la diplomática en Luciana Duranti y Kenneth Thibodeau (2006), "The Concept of Record in Interactive, Experiential and Dynamic Environments: the View of InterPARES", *Archival Science* 6(1), pp. 15-21.

método, utilizado de manera menos frecuente, para confirmar la identidad y la integridad se basa en la comparación. Los documentos de archivo de un fondo se comparan con las copias remitidas y mantenidas por fuentes externas en el curso normal del negocio del creador.

Los documentos de archivo creados y mantenidos utilizando tecnología digital presentan dificultades adicionales y los archiveros aún no han desarrollado prácticas normalizadas para ponderar la autenticidad en este entorno. Las cuestiones giran en torno al hecho de que los objetos digitales se duplican, se distribuyen, se renombran, se reformatean y se convierten con facilidad, así como a la posibilidad con la que pueden ser falsificados sin dejar traza. Los siguientes ejemplos ilustran el grado de pérdida para los archiveros, los historiadores, los abogados y otros que requieren documentos auténticos de archivo en su trabajo:

- El soporte físico sobre el que los documentos digitales se almacenan ha perdido en gran medida su significatividad, para confirmar la fecha de un documento de archivo o su lugar de fabricación. Cualquiera con acceso a equipamiento y soportes de almacenamiento obsoletos y en funcionamiento tiene capacidad para copiar ficheros digitales, por ejemplo, a cintas de 9 pistas o disquetes de 5-1/4 pulgadas.
- El sello de fecha sobre cualquier fichero digital puede modificarse ajustando el reloj del sistema.
- Pocas instituciones comprendieron qué hacen sus empleados una vez que se les confía *software* de procesamiento de texto. Los formularios normalizados de documentos, como memorandos y correspondencia con membrete, desaparecieron bajo el embate de formas de documentos de archivo nuevas e individualizadas, que incluían con rapidez colores, gráficos e incluso efectos de sonido

personalizados, así como la atribución de nuevo significado al uso de mayúsculas y minúsculas, los colores y el desarrollo de emoticonos. El grado de erosión de las prácticas de creación de documentos de archivo normalizados varió, enormemente, entre tipos y tamaños de organizaciones corporativas y gubernamentales.

- La introducción de redes de correo electrónico permitió que los documentos de archivo viajaran por muchas rutas nuevas entre el personal, fuera de las rutas de distribución de procedimientos tradicionales de oficina bien establecidas.
- Las severas reducciones en personal de administración de documentos de archivo en muchas organizaciones, fue estimulada por la asunción de que los objetos digitales no tenían que ser gestionados, de alguna manera, creando estragos en los fondos de la Oficina de Documentos de Archivo, que en gran medida dejó de recibir los documentos de archivo creados y transmitidos en forma digital.

Cuando valoramos documentos de archivo creados en un entorno digital, la ponderación de la autenticidad de los documentos de archivo debe devenir un proceso más abierto y flexible, ejecutado y documentado por el preservador. La cadena sin rupturas de custodia, el conocimiento de las prácticas de gestión de documentos y la verificación puede que aún ofrezcan algunas garantías de autenticidad. A éstos debe añadirse, ahora, la verificación de la conformidad con cada uno de los requisitos de cota para la autenticidad.

Documentar la ponderación de la autenticidad

El informe de valoración debería documentar los controles puestos en vigor por el creador para garantizar la identidad y

la integridad de los documentos de archivo y así la presunción de su autenticidad. Estos controles incluyen cada uno de los requisitos de cota que apoyan la presunción de autenticidad.[38] Brevemente, éstos incluyen:

A.1. Expresión de los Atributos del Documento de Archivo y Vínculo al Documento de Archivo (por ejemplo, metadatos de identidad y de integridad).
A.2. Privilegios de Acceso.
A.3. Procedimientos de Protección contra Pérdida y Corrupción de los Documentos de Archivo.
A.4. Medidas de Protección contra el Deterioro de los Soportes y el Cambio Tecnológico.
A.5. Establecimiento de Formas Documentales.
A.6. Autenticación de Documentos de Archivo.
A.7. Identificación del Documento de Archivo Autorizado.
A.8. Retirada y Transferencia de la Documentación Relevante.

Supervisar los documentos de archivo identificados para su preservación a largo plazo

Una vez que la valoración se ha completado, los documentos de archivo identificados para su preservación deben supervisarse a intervalos regulares hasta el momento en que sean transferidos al preservador. La supervisión implica confirmar con el creador de los documentos de archivo que nada ha cambiado con respecto al modo en que las clases de documentos de archivo identificadas para su transferencia se han creado o mantenido; o si han tenido lugar cambios, que no han afectado a la naturaleza y los atributos de los documentos de archivo, su valor, su autenticidad o la viabilidad de su preservación.

[38] Véase Apéndice 21a.

Muchos cambios dentro de una organización pueden afectar a la supervivencia permanente de los documentos digitales de archivo. La posibilidad de que sean destruidos en un instante es mucho mayor que para los documentos de archivo tradicionales. Este peligro queda compensado en algo por la tendencia a duplicar materiales de manera incontrolada. Desafortunadamente, si la producción de copias no está controlada, es improbable que alguien se dé cuenta de cuándo es destruida la última copia de un documento de archivo.

El escenario más simple puede implicar una actualización del sistema, ya sea de *hardware* o de *software*, que afectará la capacidad para aceptar los documentos de archivo. Una actualización también podría dar como resultado un rediseño incluso menor del sistema, que podría eliminar la capacidad de separar documentos de archivo temporales de aquellos que deben ser retirados para su transferencia al preservador.

Un segundo escenario puede implicar cambios en el mandato o las funciones de una organización. Esto puede conducir fácilmente a cambios en el modo en que se usan las aplicaciones informáticas, así como la naturaleza y la cantidad de datos que contienen. Puede que las personas responsables del rediseño del sistema no sean conscientes del requisito de transferir los documentos de archivo existentes al preservador designado antes de que el sistema pueda ser modificado. Sin intervención, incluso la documentación acerca de la aplicación original y las cintas de copia de seguridad se desplazará inexorablemente hacia una fecha de destrucción programada.

Finalmente, el colapso generalizado de adecuadas prácticas de administración de documentos de archivo en la mayoría de las organizaciones significa que los documentos de archivo se identifican de manera pobre y se almacenan incorrectamente en localizaciones no seguras. Puede que los administradores

–e incluso los administradores de documentos de archivo–, no comprendan los detalles de la infraestructura técnica, mientras que es probable que el personal de TIC no esté familiarizado ni con la historia de una organización ni con la importancia relativa de los documentos de archivo más antiguos en diversos almacenes de datos. Puede que los discos duros se limpien, las cuentas de usuario y todos los ficheros que contienen pueden borrarse; las cintas y los discos pueden reciclarse o destruirse; y quizá se deseche la tecnología de reproducción obsoleta para satisfacer los requisitos cotidianos de rapidez y eficacia, sin conocimiento del impacto de tales acciones sobre los documentos de archivo de una organización o sobre los acuerdos de transferencia pre-existentes diseñados para asegurar su preservación a largo plazo.

Actualizar las valoraciones

También tienen que actualizarse a intervalos regulares, aunque de manera menos frecuente de lo que tienen que supervisarse los documentos de archivo identificados para su transferencia. La información reunida durante una visita de supervisión puede proporcionar la primera indicación de que se requiere una nueva valoración. El cambio dentro de las organizaciones y dentro de sus sistemas de creación de documentos de archivo y de gestión de documentos es inevitable. Los mandatos y las responsabilidades organizacionales pueden cambiar, así como el modo en que esas obligaciones se llevan a cabo; y a los datos acumulados en los sistemas existentes se les puede dar nuevos usos, que podrían incrementar su valor a largo plazo. Al nivel más simple, los sistemas que inicialmente no contenían documentos de archivo pueden actualizarse para que sí los tengan. Esto es particularmente cierto durante este periodo de sistemas de gestión de documentos "híbridos", en el que los sistemas de documentos de archivo basados en papel siguen coexistiendo con las primeras etapas de sistemas de información, documentos o documentos de archivo digitales.

Identificar todos los componentes digitales[39]

Los documentos de archivo en papel mantenidos en sistemas tradicionales de gestión ofrecen generalmente un paquete firmemente encapsulado, en el que el contenido del documento de archivo está sólidamente unido a su soporte papel y el documento de archivo mismo está contextualmente archivado con los documentos de archivo relacionados. Este sistema sin fisuras comenzó a romperse con la introducción de la tecnología, cuando, por ejemplo, los negativos fotográficos tenían que procesarse para producir impresos y las imágenes en movimiento resultaban de múltiples capas de sonido e imágenes, combinadas y re-combinadas para producir la impresión compuesta final que se proyecta en los cines o se emite en televisión.

Posteriormente, la tecnología digital ha desmantelado el documento de archivo en una serie de componentes. Para extraer con éxito los documentos digitales de archivo del sistema en el que fueron creados –o incluso desde un sistema secundario de mantenimiento–, el preservador debe asegurar que todos los componentes digitales esenciales están identificados y que las relaciones implícitas se hacen explícitas en los metadatos antes de que se transfiera todo el constructo. Uno de los ejemplos más comunes de un componente digital es la biblioteca de fuentes, cierto número de las cuales puede ser seleccionada por el creador para ser usado en la presentación de un documento realizado con procesador de textos. En *Windows*, éstas se almacenan en ficheros .dll (biblioteca de vínculos dinámicos). Para que el preservador sea capaz de reproducir este documento de archivo de modo que refleje las intenciones

[39] Un componente digital se define como "Un objeto digital que es parte de uno o más documentos digitales, y los metadatos necesarios para ordenar, estructurar o manifestar su contenido y su forma, requiriendo una acción de preservación dada" (InterPARES 2 *Terminology Database*, *op. cit.*).

originales del creador, tanto el componente digital que contiene el texto como el componente digital que contiene la fuente deben haber sido preservados, así como el vínculo entre ellos, establecido de tal modo que el *software* que intente visualizar el contenido del fichero de texto pueda encontrar la adecuada biblioteca de fuentes.[40]

Determinar la viabilidad de la preservación

Aunque no es parte de la ponderación del valor de los documentos de archivo, el proceso de valoración debe ser completado con una investigación cuidadosa acerca de los requisitos de preservación técnica para la preservación. Diferentes estrategias de preservación (véase Apéndice 21c, sección B) pueden variar ampliamente en coste y pueden producir resultados muy diferentes. Un documento de archivo textual despojado de todo su formateo puede ser aceptable en una situación en la que el preservador esté interesado en resguardar sólo el contenido del documento de archivo. Sin embargo, si el significado está determinado por la forma documental y por las características de visualización del documento de archivo, se requerirá una solución de preservación más compleja.

Una determinación de la viabilidad de la preservación es esencial si el cuerpo preservador ha de comprender claramente el costo de la adquisición y la preservación con las que se está comprometiendo. Esto no es una actividad nueva; es simplemente la extensión al ámbito digital de la identificación de los recursos necesarios para preservar, por ejemplo, documentos de archivo en papel que están mohosos o carretes de imagen

[40] Una descripción más detallada del "componente digital", con ejemplos adicionales que ilustran el concepto, está disponible en Preservation Task Force (2001), "Appendix 6: How to Preserve Authentic Electronic Records", en Duranti, *Long-term Preservation*, *op. cit.*, pp. 293–328. Reimpresión en línea disponible en http://www.interpares.org/book/interpares_book_o_app06.pdf.

en movimiento que se han reducido mal. El estado actual de la preservación de hoy en día implica, sin embargo, que los costos de preservación deben considerarse como recurrentes. El recopiado de fondos de un soporte físico a otro se requerirá tan a menudo como el formato seleccionado devenga obsoleto. La conversión de formatos de fichero se requerirá cuando la obsolescencia lógica amenace con volver el contenido en ilegible. Además, puede que los documentos digitales de archivo considerados para su preservación a largo plazo requieran medidas demasiado complejas para el entorno tecnológico y los recursos de conocimiento de la organización preservadora; y esto podría implicar el aplazamiento de la transferencia.

Adquirir los documentos de archivo seleccionados para su preservación permanente

La actividad del preservador de adquirir los documentos de archivo seleccionados, y todas las actividades de preservación que se siguen de ella, tienen como fin la autenticidad y la accesibilidad continuadas de aquellos documentos de archivo que se han seleccionado para su preservación continuada. Este movimiento de los documentos de archivo, desde la custodia del creador (o su sucesor legítimo) a la custodia del preservador, es una coyuntura crítica en la cadena de preservación y debe hacerse con gran cuidado para asegurar que nada se ha desviado en el proceso de transferencia.

Desarrollar un plan compartido para la transferencia

Una transferencia con éxito desde el actual custodio de los documentos de archivo (sea su creador original o su sucesor legítimo), a la organización o programa que adopta la responsabilidad de la preservación a largo plazo, requiere un plan acordado por ambas partes. Reacceder a sistemas obsoletos o extraer documentos de archivo inactivos de sistemas en

funcionamiento implicará definitivamente costos en recursos humanos para el tiempo de copia y, potencialmente, para el tiempo de programación. Puede que también se requieran *hardware* y *software* especiales. Los formatos lógicos y físicos (o virtuales), usados para la transferencia, deben ser aceptados por ambas partes. Como regla general, el plan de transferencia debería desarrollarse cuando la viabilidad técnica de la adquisición y la preservación se emprenda. Si las dos partes no pueden llegar a un acuerdo sobre el proceso de transferencia, puede que la decisión de valoración tenga que revisitarse. De nuevo, en este periodo de gestión híbrida de documentos, puede que aún existan opciones basadas en papel y microfilm. De manera alternativa, el preservador podría animar al creador de los documentos de archivo a adoptar actualizaciones al sistema de documentos de archivo que permitan transferencias regulares más fáciles.

Hacer cumplir procedimientos normalizados

Los controles sobre la transferencia de los documentos digitales de archivo desde la custodia del creador a la del preservador deben incluir:

- Establecer, implantar y supervisar procedimientos para registrar la transferencia de los documentos de archivo.
- Verificar la autoridad de la transferencia.
- Examinar los documentos de archivo para determinar si se corresponden con los documentos de archivo que se han designado para su transferencia.
- Acceder a los documentos de archivo.

Como parte del proceso de transferencia, la autenticidad de los documentos de archivo del creador, que fue ponderada

como parte del proceso de valoración, debería verificarse. Esto incluye verificar que los metadatos relacionados con la identidad y la integridad de los documentos de archivo han sido transferidos junto con los documentos de archivo relacionados y que están vinculados a ellos; y que están acompañados por cualquier información relevante acerca del entorno técnico y administrativo en el que fueron creados y mantenidos.

Mantener el formato lógico más antiguo disponible

El formato lógico[41] en el que los documentos de archivo fueron creados originalmente, o en el que fueron mantenidos por el creador en el momento de la transferencia, debería, siempre que sea viable, mantenerse por parte del preservador, además de cualquier copia de preservación o de referencia generada después de la transferencia. Deberían seleccionarse estrategias de preservación, como una trayectoria específica de conversión, fallos a la largo del tiempo. La custodia continuada del formato lógico inicial permitirá al preservador reiniciar esencialmente el proceso de preservación con la copia más autorizada de los documentos de archivo, aplicando una estrategia de preservación diferente a los documentos de archivo. Durante los largos periodos durante los cuales los preservadores mantienen documentos de archivo, puede que la experiencia muestre que otras estrategias de preservación son más estables a lo largo del tiempo o se puedan sacar adelante de manera más fácil a largo plazo. De manera alternativa, puede que se hayan desarrollado nuevos métodos de preservación después de la adquisición y el procesamiento inicial de los documentos de archivo.

[41] Formato lógico se define como "La ordenación organizada de datos sobre soporte electrónico que asegura que las estructuras de control de ficheros y datos son reconocibles y recuperables por el sistema operativo del ordenador que los aloja" (InterPARES 2 *Terminology Database*, *op. cit.*). Dos formatos lógicos comunes para ficheros y directorios son ISO 9660 para CD-ROM, y Universal Disk Format (UDF) para DVD.

Evitar duplicados

A causa de la facilidad de replicación de los documentos digitales de archivo, el preservador debe tener en vigor procedimientos para asegurar que los documentos digitales de archivo de una serie específica son transferidos por un creador específico al preservador sólo una vez. Una información exacta sobre la identidad es un primer paso importante para evitar la duplicación de esfuerzos por parte del creador y del preservador. Además, si el preservador proporciona copias de referencia al creador después de la transferencia de los documentos de archivo, deberían identificarse claramente y marcarse como tales para impedir la retransferencia accidental.

Documentar todo el procesamiento

Los procesos iniciales aplicados durante e inmediatamente después de la transferencia puede que estén, o no, relacionados con la preservación en sí. Confirmar la identidad de los materiales transferidos, revisarlos en busca de virus y confirmar la completitud de los ficheros son procedimientos que tienden a dejar el fichero transferido sin cambios. La conversión de ficheros, el renombrado de objetos digitales y el encapsulamiento de ficheros son actividades más intrusivas. En ambos casos, los preservadores deben documentar todo el procedimiento de los documentos digitales de archivo y los efectos del procesamiento mientras los documentos de archivo están bajo su custodia (véase Apéndice 21b, requisito B.2). Esta documentación debe incluir información de:

- Por qué se aplicaron ciertos procesos a los documentos de archivo.
- Qué documentos de archivo fueron procesados.
- La fecha en que el proceso fue ejecutado.
- Los nombres de las personas que ejecutaron y documentaron los diversos pasos del (de los) proceso(s).

- El impacto del proceso ejecutado sobre la forma, el contenido, la accesibilidad y el uso de los documentos de archivo.
- La descripción de cualquier daño, pérdida u otros problemas encontrados como resultado del procesamiento, incluido cualquier efecto sobre los elementos que expresan la identidad y la integridad de los documentos de archivo.

El preservador tendría que producir copias de los documentos de archivo adquiridos. Es importante recordar que éstas deberían producirse en un entorno que satisfaga los requisitos relevantes[42] de los Requisitos de Cota que Apoyan la Presunción de Autenticidad de los Documentos Electrónicos de Archivo de InterPARES 1.

Preservar los documentos de archivo ingresados

El preservador designado de los documentos de archivo es la entidad responsable de adoptar la custodia física y legal; y preservar, proteger y asegurar el acceso continuado a los documentos de archivo de un creador. Sea una organización externa o una unidad interna, el papel del preservador designado debería ser el de un custodio fiable[43] de los documentos de archivo del creador. Las copias auténticas de los documentos de archivo del creador son mantenidas por el custodio fiable en un *sistema de preservación fiable* (véase Apéndice 21c), que

[42] Establecer formas documentales. Si el creador establece la forma documental del documento de archivo, usualmente no se aplicaría al preservador, excepto si la forma documental original del documento de archivo se ha perdido y el preservador debe especificar un sustituto para permitir el acceso.

[43] Un custodio fiable se define en la Base de Datos de Terminología de InterPARES 2 como "Un preservador que puede demostrar que no tiene motivo para alterar los documentos de archivo preservados o para permitir que otros los alteren, y que es capaz de implantar todos los requisitos para la preservación auténtica de documentos de archivo" (InterPARES 2 *Terminology Database, op. cit.*).

debería incluir en su diseño un sistema de descripción y recuperación. Este sistema de preservación fiable también debe tener en vigor reglas y procedimientos para la producción permanente de copias auténticas cuando el sistema existente devenga en obsoleto y la tecnología se actualice.

Describir los documentos de archivo

La información acerca de los documentos de archivo y sus contextos recogida durante las etapas de valoración y procesamiento debería formar parte de la descripción archivística del fondo o la serie a los que los documentos de archivo pertenecen (véase Apéndice 21b, requisito B.3). Esto también debería incluir información acerca de los derechos de propiedad intelectual o problemas de privacidad.

La descripción archivística del fondo o la serie que contiene los documentos digitales de archivo debería incluir –además de información acerca de los contextos jurídico-administrativos, de procedencia, procedimental y documental de los documentos de archivo– información acerca de los cambios que han tenido los documentos digitales de archivo del creador desde que se crearon por primera vez. La descripción también debería incluir una visión general de los procesos de transferencia y preservación basada en la documentación discutida en la sección 3.5 y la explicación de las relaciones entre componentes digitales discutida en la sección 2.7.

Identificar las ramificaciones legales de las acciones de preservación

Cuando se selecciona una estrategia de preservación, deberían revisarse sus implicaciones legales. Por ejemplo, la conversión de formato de un entorno propietario podría implicar al preservador en acciones ilegales. En los Estados Unidos, la Digital

Millennium Copyright Act convirtió en delito producir herramientas que puedan esquivar las medidas de protección del copyright. A nivel internacional, el Tratado de Copyright de la Organización Mundial de la Propiedad Intelectual (WIPO WCT) contiene provisiones que incluyen la protección del copyright del *software*, así como de las obras digitales; e introduce sanciones criminales por su infracción, que abarca desde la copia no autorizada de material ubicado en un sitio web hasta la retirada o la alteración de los controles de gestión de derechos de las obras digitales. La mayoría de paquetes de *software* también incluyen algún tipo de restricción similar, con la que los usuarios deben estar conformes durante el proceso de instalación.

Confirmar la eficacia de la estrategia de preservación seleccionada

Como se discutió en la sección 2.8, ahora existe un cierto número de estrategias de preservación disponibles. Idealmente, la estrategia de preservación seleccionada debería probarse sobre los documentos de archivo antes de la transferencia formal al preservador, para asegurar que funcionará como se espera. De manera realista, la mayoría de organizaciones o programas de preservación sólo pueden financiar este tipo de pruebas de manera excepcional. Así como los conservadores tradicionales prueban cuidadosamente los tratamientos propuestos antes de aplicarlos en masa a los documentos analógicos de archivo, los preservadores digitales deben estar constantemente alerta con respecto al impacto que cada proceso de preservación puede tener sobre los documentos de archivo y asegurarse que es la elección adecuada para preservar documentos de archivo auténticos. Los defectos en la aplicación de *software* y las variaciones de funcionalidad de las versiones a lo largo del tiempo pueden dar como resultado consecuencias inesperadas cuando se aplican a un nuevo grupo de documentos de archivo.

Parte de este proceso incluye una constante consciencia de la necesidad de rastrear la presencia y el funcionamiento de todos los componentes digitales. Un cambio en un componente puede tener resultados inesperados en un segundo componente, alterar el modo en que funciona la relación entre dos partes esenciales del documento de archivo, o afectar a la capacidad de interactuar de estos componentes. Una relación diferente que podría resultar afectada es la que existe entre los miembros de un grupo relacionado de documentos de archivo, como un *dossier* o una serie; y la presentación de esa agregación en el orden correcto (por ejemplo, alfabético, cronológico o jerárquico). Si el orden original se ha perdido, habrá que adoptar medidas correctoras.

Mantener un almacenamiento adecuado

Conservar un entorno de almacenamiento adecuado (temperatura y humedad relativa) es un principio extensamente aceptado de la preservación archivística. Para los materiales que se están almacenando es la contribución más eficaz en costos para la preservación a largo plazo de los documentos de archivo. Los fabricantes de soportes de almacenamiento magnéticos u ópticos ofrecen por regla general recomendaciones acerca de las condiciones de almacenamiento óptimas. El entorno debe ser supervisado constantemente y los lectores deben comprobarse de manera regular. Esta recomendación es una de las ocho estrategias obligatorias de mantenimiento delineadas en la sección 1.7 y discutidas en el Apéndice 21c, sección A.

Dar salida a los documentos de archivo

Como se hizo notar anteriormente, la accesibilidad continua (es decir, el uso) es una parte integral del proceso archivístico. En consecuencia, proporcionar acceso a los documentos de archivo preservados es un componente esencial en la cadena

de preservación. Debería ser gestionado por el preservador con el mismo sentido de la responsabilidad y el mismo grado de competencia técnica o profesional impartida a la valoración, la adquisición y transferencia, la descripción y el almacenamiento de los documentos de archivo.

Explicar el modo en que se realizaron las copias de referencia

La relación entre los documentos de archivo adquiridos del creador y cualquier copia producida por el preservador debe quedar claramente descrita e inmediatamente accesible a los usuarios (véase Apéndice 21b, requisito B.2.b). Esto también debería incluir documentar el modo en que las medidas de control del proceso de reproducción que están en vigor fueron establecidas e implantadas y el modo en que se supervisan para asegurar que el contenido de los documentos de archivo reproducidos no ha cambiado en el curso de la reproducción. Puede que las copias de documentos de archivo del sistema de preservación del preservador no sean designadas como auténticas si el preservador las ha realizado con propósitos distintos al de preservación; por ejemplo, puede que se realice una copia de la que se han retirado los identificadores personales a efectos de acceso.

Documentar el proceso de reproducción de los documentos de archivo y sus efectos es un medio esencial para demostrar que el proceso de reproducción es transparente (por ejemplo, libre de simulación o engaño). Tal transparencia es necesaria para la satisfacción eficaz del papel del preservador como un custodio fiable de los documentos de archivo. También proporciona a los usuarios de los documentos de archivo una herramienta crítica para ponderar e interpretar los documentos de archivo demostrando su autenticidad continuada y proporcionando una historia completa de ellos, dentro de la cual, la historia de la reproducción es una parte esencial.

Expresar los requisitos técnicos para el acceso

Como se mencionó en la sección 1.1 diferentes preservadores proporcionan servicios de referencia a diferentes tipos de usuarios. Esto afectará a los formatos de referencia y a los mecanismos adoptados por la organización o el programa de preservación, requiriendo métodos más sencillos para miembros del público general que quizás no tengan una computadora o posean una máquina bastante simple con unas pocas piezas normalizadas de *software*. Para satisfacer las necesidades de estos usuarios, es posible que el preservador tenga que emprender un procesamiento adicional o crear herramientas especializadas para ayudar a los investigadores. Es más probable que los usuarios tecnológicamente más expertos –como los estadísticos que realizan análisis de datos o los forenses que llevan a cabo investigaciones sobre fraude–, apliquen sus propias herramientas de *software* a las copias de los documentos de archivo.

Conclusión

Este documento ha delineado una serie de recomendaciones para instituciones, organizaciones y programas con responsabilidades de preservación para documentos digitales de archivo de los que se puede presumir que son auténticos y exactos mientras están bajo la custodia del preservador. Para preservadores individuales y organizaciones de preservación pequeñas, la carga puede parecer grande, pero la alternativa —pérdida de documentos de archivo o la emergencia de documentos de archivo corruptos y no auténticos—, sería un problema incluso mayor a la larga. Las organizaciones pequeñas se beneficiarán de llevar a cabo una clara designación del individuo o de los individuos responsables de supervisar la preservación de los documentos digitales de archivo de la organización. Llévese en mente, sin embargo, que no todas las recomendaciones presentadas en este documento tienen que implantarse en cada circunstancia;

cada preservador debería ser capaz de seleccionar y adoptar las medidas que abordan sus problemas particulares en el contexto específico en el que funciona. Puede que también se den casos en los que sean necesarias medidas adicionales a causa de requisitos legislativos o reguladores específicos de la jurisdicción administrativa o cultural del preservador. En tales casos, puede que se requiera consultoría con expertos legales. Los individuos, las oficinas y las pequeñas organizaciones responsables de la preservación no deberían dudar en contactar a tales expertos en busca de consejo sobre cualquier cuestión relativa a la preservación de los documentos digitales de archivo bajo su custodia y bajo su control.

Apéndice E: Plantilla para establecer la concordancia entre los requisitos de autenticidad y los elementos de la política

Revise los elementos requeridos para la autenticidad y la preservación a largo plazo de los documentos digitales de archivo en la primera columna. Establezca una concordancia entre cada elemento y una cláusula o párrafo de sus ya existentes políticas de documentos de archivo (columna 2). Identifique los elementos que deben estar incluidos en la política de preservación digital en desarrollo, para asegurar que están incluidos todos los elementos necesarios.

Elementos necesarios para la autenticidad	Representados en las políticas existentes	Requeridos en la nueva política en desarrollo
Accesibilidad • Elija *software* y hardware para la interoperabilidad. • Elija *software* que sea retrospectivamente compatible. • Adopte normas de *software* oficiales o *de facto*. • Documente completamente todas las elecciones y cualquier personalización. • Elija formatos extensamente utilizados, no propietarios, independientes de la plataforma, no comprimidos y con especificaciones libremente disponibles siempre que sea posible. • Elija compresión sin pérdida cuando se requiera compresión.		

Fijeza • Los documentos digitales de archivo deberían tener forma fija y contenido estable. • La forma documental debe retenerse como original (fija dentro de los confines del sistema). • Dote a los documentos de archivo de variabilidad limitada (reglas establecidas para la selección del contenido y la forma documental que permitan variaciones conocidas y estables). • Establezca los elementos esenciales intrínsecos y extrínsecos de cada presentación o forma documental.		
Identidad • Asegure la completitud de los metadatos de identidad: • Nombres de personas (autor, redactor, generador, destinatario, receptor). • Título/asunto (acción o materia). • Forma documental (carta, informe, y otros). • Presentación digital (formato, contenedor, codificación, y otros). • Fechas de creación y transmisión. • Expresión del contexto documental (por ejemplo, código de clasificación, carpeta o directorio, y otros). • Indicación de adjuntos (si es aplicable). • Indicación de copyright u otros derechos de propiedad intelectual (si es aplicable). • Indicación de la presencia o retirada de firmas digitales.		

• Indicación de otras formas de autenticación (por ejemplo, corroboración, testimonio, y otros). • Número de borrador o versión (si es aplicable). • Existencia y localización de materiales duplicados fuera del sistema (indique cuál es la copia autorizada).		
Integridad • Asegúrese de que todos los materiales digitales contienen información que ayudará a verificar su integridad. • Confirme la completitud de los metadatos de integridad: • Nombre de la persona/oficina que los trata. • Nombre de la oficina o persona con responsabilidad primaria para mantenerlos (puede ser la misma que la de tratamiento). • Indicación de anotaciones. • Indicación de cambios técnicos a los materiales o a la aplicación. • Restricciones de acceso (si es aplicable). • Privilegios de acceso (si es aplicable). • Documento de archivo vital (si es aplicable). • Disposición planificada.		
Organización • Organice los materiales digitales en agrupamientos lógicos (cuadro de clasificación, metadatos de identidad).		

Autenticación • Use técnicas de autenticación que fomenten el mantenimiento y la preservación de los materiales digitales. • Independiente de la tecnología *vs.* dependiente de la tecnología.		
Protección • Proteja los materiales digitales de acciones no autorizadas.		
Copia de seguridad • Proteja los materiales digitales de pérdida y corrupción accidentales. • Desarrolle una rigurosa política o rutina que asegure que se hace copia de seguridad diaria de su sistema. • Elija e instale la mejor tecnología de copia de seguridad para su situación.		
Obsolescencia • Emprenda pasos contra la obsolescencia del *hardware* y del *software*.		
Conciencia		

Apéndice F: Ejercicio 1. Puntos de discusión

Fortalezas

- El lenguaje es claro y conciso.
- La política está basada en sus contextos administrativo y jurídico, haciendo referencia a las políticas de la universidad y a la legislación relevante.

Debilidades

- La sección Alcance sólo declaraba qué documentos de archivo están sujetos a la política, pero no especifica qué individuos o departamentos están sujetos a la política.
- La sección Declaración de política incluye información que es dependiente de la tecnología y que estaría mejor contenida en un documento de guía o procedimental.
- Falta información que debería estar contenida en las secciones: Definiciones, Información de contacto y Control de versiones.

Apéndice G: Ejercicio 2. Puntos de discusión

¿Política o recomendación? Este documento es identificado como política y recomendación; y es ambiguo en su propósito. Tal y como está escrito no es ejecutable.

Roles y responsabilidades

La sección 1.1 establece que la "recomendación" es para los propietarios de los documentos de archivo, los administradores de TIC y los funcionarios o usuarios. ¿Cómo define esta política a los propietarios de los documentos de archivo? Los propietarios de los documentos de archivo y los administradores de TIC no tienen las mismas responsabilidades y éstas deberían delinearse separadamente. La sección de papeles y responsabilidades omite cualquier referencia a los funcionarios o usuarios. ¿Cuál es su papel en la implantación de esta política? Todas las partes interesadas responsables de implantar la política tienen que identificarse y sus funciones y responsabilidades tienen que delinearse.

Definiciones. La sección de definiciones tal y como existe actualmente no es lo suficientemente comprehensiva como para asegurar que la política puede seguirse y ejecutarse. Los conceptos de metadatos, valoración, destrucción, autenticidad y valor archivístico; sistemas de información de negocio y sistemas de gestión de documentos deberían incluirse en la sección de definiciones.

Sección de alcance. Aclara el alcance de la política e identifica la medida de los documentos de archivo cubiertos por la política y los grupos de interesados responsables de su implantación.