2º Encuentro Universitario de Ingeniería de Software y bases de Datos

Cd. Universitaria,

Octubre 28 de 2015

“Preservación de archivos digitales confiables”

Juan Voutssás M.

Investigador; Instituto de Investigaciones Bibliotecológicas y de la Información (IIBI), Universidad Nacional Autónoma de México (UNAM)

Director del TEAM Latinoamérica del Proyecto InterPARES (The International Research on Permanent Authentic Records on Electronic Systems

Desafíos de los Documentos de Archivos Digitales:

1) **Preservarlos a pesar de los cambios y la obsolescencia tecnológica**

2) **Preservarlos auténticos, íntegros y confiables**

Conservación y preservación de documentos de archivo digitales

Mantenimiento: Tiene que ver con el soporte y forma del documento de archivo, y su alcance es siempre el corto-mediano plazo. Sinónimo de “conservación”.

Preservación: Tiene que ver con el contenido del documento de archivo, y su alcance siempre es el largo plazo.

Conservación y preservación de documentos de archivo digitales:

Conservación documental digital: “Acciones tomadas para anticipar, prevenir, detener o retardar el deterioro del soporte de documentos digitales con objeto de tenerlos permanentemente en condiciones de usabilidad, así como la estabilización tecnológica, la reconversión a nuevos soportes, sistemas y formatos digitales para garantizar la trascendencia de sus contenidos”.

Preservación documental digital es a la vez un objetivo y un resultado: como objetivo, “preservación” es “el aseguramiento a largo plazo de la permanencia y acceso del contenido de documentos digitales confiables a lo largo del tiempo y las tecnologías”. Al aplicar la conservación y lograr este objetivo se obtiene como resultado –se logra– la preservación de los materiales; esto es: se obtiene la “protección del contenido intelectual de materiales –datos, documentos o archivos–”. Glosario InterPARES

1) Preservarlos a pesar de los cambios y la obsolescencia tecnológica

Características críticas de los documentos de archivo digitales:

- No existen como entidades físicas, están constituidos por componentes digitales vinculados (el documento de archivo “manifiesto” no tiene la misma naturaleza que el documento de archivo “almacenado”)

- Sin tratamiento, la obsolescencia tecnológica hace que los documentos sean inaccesibles en un lapso muy corto, a pesar de que permanezcan. Por lo mismo, no podemos dejar sus cadenas de bits inamovibles eternamente; esto los llevaría a ser inaccesibles con el tiempo. Para poder preservarlos, debemos cambiarlos de tiempo en tiempo.

- A pesar de ese cambio, debemos ser capaces de afirmar que se mantienen auténticos, íntegros, exactos y confiables, ya que:

 * Se ha conservado su forma fija y su contenido estable;

 * Tienen información que ayuda a verificar su identidad e integridad;

 * Se han protegido de acciones no autorizadas;

 * Se han protegido de pérdida o corrupción accidental.

Características críticas de los documentos de archivo digitales:

-No es fácil identificar la versión final, oficial, fiable y precisa.

-Su naturaleza de acceso electrónico y remoto dificulta proteger la propiedad intelectual y la privacidad.

- Es frecuente que existan sistemas de gestión de documentos de archivo digitales que contienen malos documentos debido a que carecen de forma fija y contenido estables, y/o de contextos identificables a través de relaciones entre ellos mismos y con otros documentos dentro y fuera del sistema.

- Deben presentar atributos (componentes intelectuales y digitales) y elementos de forma claramente definidos.

Deben establecerse estrategias de conservación y preservación

Estas estrategias se basan en general en normas y *modelos de aproximación;* el cimiento de todas ellas es la norma:

“ISO/IEC 15489:2001 *Información y Documentación − Gestión de Documentos − Parte 1. Generalidades”* y la norma ISO/IEC 15489:2006 *"Información y Documentación − Gestión de documentos − Parte 2: Directrices”.*

El propósito de ellas consiste en ser una guía para la gestión de documentos de archivo de una organización, sea cual sea su soporte.

Establecen que ***“...los documentos de archivo deben ser auténticos, confiables, completos, sin alteración, y deben permitir su uso y acceso. Asimismo, deben poseer metadatos que definan el contexto, contenido y estructura y deben reflejar con precisión la comunicación, acción o decisión...”***

Otros modelos de aproximación útiles

El "*Modelo de Referencia de Sistemas de Información de Archivo Abierto*", OAIS u "Open Access Information System", desarrollado por el CCSDS, Consejo integrado por miembros de diversas organizaciones asociadas para crear protocolos estandarizados, estándares abiertos de comunicación de datos, etc. Este es un "modelo lógico" o práctico que trata la manera en que los documentos digitales deben ser preparados, enviados a un archivo, almacenados durante periodos largos, conservados y recuperados. Está construido alrededor de seis entidades o funciones de alto nivel que describen las grandes actividades que incidirán positivamente para la preservación de cierta información: ingesta de la información, su gestión, almacenamiento, administración del archivo, plan de preservación, y acceso o diseminación de la información.

OAIS - *"Reference Model for an Open Archival Information System" 2012.* Versión CCSDS 650.0-M-2. Management Council of the Consultative Committee for Space Data Systems (CCSDS). Washington DC, June 2012, 148 p. Disponible en: http://public.ccsds.org/publications/archive/650x0b1.pdf

Otros modelos de aproximación útiles

MoReq -Modelo de requisitos para la gestión de documentos de archivo- muy difundido en ese continente. Fue elaborado por la Comisión Europea a través de su programa IDABC -*Interoperable Delivery of European e-Government Services to public Administrations, Business and Citizens*- de gestión de documentos electrónicos de archivo. Este no es un modelo de preservación en sí; consiste en un modelo que se centra en la estandarización de los requisitos funcionales para la gestión de documentos electrónicos de archivo a fin de normalizar esta gestión en todos los países miembros de la unión europea así como por todos los interesados en el desarrollo y aplicación de sistemas de gestión de documentos electrónicos de archivo -archivistas, informáticos, proveedores de servicios, instituciones académicas, etc.

Moreq - "Modelo de Requisitos Para la Gestión de Documentos Electrónicos de Archivo" 2001. DLM Forum. Véase también: M*oreq2 - Modelo de Requisitos Para la Gestión de Documentos Electrónicos de Archivo, versión 2*. 2004. Y también: *MoReq 2010 - Modelo de Requisitos Para la Gestión de Documentos Electrónicos de Archivo*, versión 2010. Disponibles en: http://ec.europa.eu/archival-policy/moreq/index_en.htm

Otros modelos de aproximación útiles

Las normas elaboradas por el Consejo Internacional de Archivos (ICA):

ISAD(G). Norma internacional general de descripción archivística. Constituye una guía general para la elaboración de descripciones de documentos de archivo.

ISDF. Norma internacional para la descripción de Funciones. Constituye una guía para elaborar descripciones de funciones de instituciones vinculadas con la producción y conservación de documentos.

Principles and Functional Requirements for Records in Electronic Office Environments. Define de manera integral principios y requisitos funcionales estandarizados para programas y aplicaciones utilizados para producir y gestionar documentos de archivo digitales en ambientes ofimáticos.

ICA – Consejo Internacional de Archivos. Disponible en:

http://www.ica.org/10207/standards/isadg-general-international-standard-archival-description-second-edition.html

Otros modelos de aproximación útiles

La "*Administración Nacional de Archivos y Documentos de Archivo*" de la unión americana -*National Archives and Records Administration o NARA*- adoptó como estándar para el manejo de archivos gubernamentales el denominado DoD.5015.2[1] del departamento de la defensa de ese país, el cual a su vez se deriva de estándares creados en la Universidad de la Columbia Británica en el Canadá.

Las especificaciones[2] establecidas por el proyecto de los Archivos Nacionales -*The National Archives*- del Reino Unido, el cual consiste principalmente en un conjunto estandarizado de requerimientos funcionales para archivos electrónicos y cuyas especificaciones cubren numerosos aspectos de la preservación de archivos de esta naturaleza.

1) "Department of Defense – Standard DoD.5015.2". USA : National Archives and Records Administration. 2003. Disponible en: http://www.archives.gov/records-mgmt/initiatives/dod-standard-5015-2.html

2) "Requirements for Electronic Records Management Systems : 2.- Metadata Standards". 2002. United Kingdom : National Archives. Disponible en: http://www.nationalarchives.gov.uk/

Otros modelos de aproximación útiles

PREMIS "PREservation Metadata: Implementation Strategies" (Metadatos de preservación: estrategias de implementación) es un proyecto del grupo conjunto de OCLC y RLG desde 2003. Consiste en un informe denominado *PREMIS Data Dictionary for Preservation Metadata* (Diccionario de datos PREMIS de metadatos de preservación) que incluye un diccionario de datos especiales para preservación, la creación de un esquema XML al efecto e información adicional sobre los metadatos de preservación.

The PREMIS Data Dictionary for Preservation Metadata". Version 2.2. 2008. Disponible en: http://www.loc.gov/standards/premis/

El modelo InterPARES:

El modelo del grupo internacional InterPARES (The International Project for Research on Permanent Authentic Records on Electronic Systems) o *Proyecto Internacional para la Investigación en Documentos de Archivo Auténticos y Permanentes en Sistemas Electrónicos* elaboró un modelo denominado *"Cadena de Preservación"* derivado del concepto "Chain of Preservation Model".

InterPARES -The International Research on Permanent Authentic Records in Electronic Systems. 2004. *"Chain of Preservation Model"*. Disponible en: http://www.interpares.org/ip2/ip2_models.cfm

El modelo InterPARES:

El modelo de la *"Cadena de Preservación"* establece que los documentos de archivo digitales deben ser cuidadosamente manejados a lo largo de toda su existencia como una secuencia que asegure que sean accesibles y legibles a lo largo del tiempo dejando su forma, contenido y relaciones intactas hasta el punto necesario que logre su continua confianza como documentos de archivo. Ello implica un control integral durante todas las fases o etapas de la existencia de los documentos de archivo desde el momento en que son producidos, continúa con una adecuada conservación por parte de su productor durante la gestión, la valoración y disposición, y finalmente durante la etapa de preservación a largo plazo como comprobantes auténticos de acciones y asuntos de los que son parte.

Estrategias

Independientemente del tipo o modelo de plan de preservación que una organización adopte, es necesario establecer unas *estrategias de conservación* y unas *estrategias de preservación*. Esto obedece de origen a planteamientos ampliamente difundidos por UNESCO en sus *Directrices para la Preservación del Patrimonio Digital* las que ofrecen un amplio marco de referencia para el establecimiento de estrategias de preservación para cada organización y sus tipos de documentos de archivo digitales (UNESCO, 2003). El establecimiento de estrategias también está estipulado como etapa importante en uno de los primeros apartados de la Norma "ISO:15489 – *Directrices*".

Estrategias de conservación

Estas estrategias tienen que ver con cuidar la duración de los soportes y mantener la accesibilidad de los documentos: **c**onsisten en un conjunto coherente de objetivos y métodos para proteger y mantener la *permanencia y accesibilidad* de los documentos de archivo digitales a lo largo de las primeras etapas de la cadena de preservación:

Selección, uso y cuidado de los soportes digitales, siguiendo estándares internacionales.

Transferencia de datos periódicamente hacia nuevos soportes digitales: ***(réplica, refrescado, migración, emulación)*** Actualización de formatos, formatos auto-contenidos, (Teoría de los Formatos Universales de Preservación)

ISO 18925:2013 "Imaging materials - Optical disc media - Storage practices"

Guidelines for Physical Digital Storage Media. Version 1.0. 2011. Libraries and Archives Canada. Sitio Oficial de la Organización. Disponible en: http://www.collectionscanada.gc.ca/

Estrategias de preservación

Estas estrategias consisten básicamente en "*un conjunto de principios, políticas, reglas y estrategias así como las herramientas y mecanismos utilizados para implementarlas y que han sido adoptadas por una institución o programa archivístico para mantener a largo plazo los componentes digitales y su información relacionada, así como para reproducir documentos de archivo auténticos y/o agregaciones de ellos que hayan sido producidos mediante la interpretación de controles externos aplicando estos últimos a los documentos de archivo seleccionados para su preservación*".

Glosario InterPARES.

Estrategias de preservación

En términos generales, las estrategias de preservación contemplan los siguientes aspectos:

- Preferir estándares[1]: en sistemas informáticos, métodos de codificación, formatos de documentos, almacenamiento físico, etc.

- Maximizar la interoperabilidad de sistemas, formatos y datos. Normalizar en lo posible.

- Usar formatos auto-descriptivos. XML + Conceptos de *"Colección de Datos por Preservación de Objeto Persistente"*, o *"Marcado Permanente con Etiquetas[2]"*, u *"Objeto digital auto-contenido de OAIS"*.

1) "Sustainability of Digital Formats". 2005. Library of Congress, USA. Disponible en: http://www.digitalpreservation.gov/formats/fdd/fdd000125.shtml

*2) **Thibodeau, Kenneth.** 2000. "Preservation and Migration of Electronic Records: The State of the Issue" En: "La conservazione dei documenti informatici - Aspetti organizzativi e tecnici"[The retention of documents - technical and organizational aspects], AIPA Seminar, 30 October 2000. Rome, Italy. Disponible en:*

http://www.interpares.org/display_file.cfm?doc=ip1_dissemination_cpnr_thibodeau_aipa_seminar_2000.pdf" \t "_blank

2) *Preservarlos auténticos, íntegros y confiables*

Con las anteriores estrategias se resuelve:

***Permanencia y accesibilidad*;**

Se requiere además

autenticidad, integridad y confianza

Autenticidad, integridad y confianza

En los documentos de archivo sobre soportes "tradicionales" las reglas de la diplomática establecen las formas en las que el estudio de los componentes del documento permiten establecer su autenticidad, integridad y confiabilidad; en su mayoría estos componentes son físicos (papel, tinta, sellos, firmas, etc.) Es decir, la autenticidad, fiabilidad, etc., y por ende confianza se establece analizando al documento en sí. Los componentes extrínsecos son evidentes también.

Autenticidad y confianza

En la diplomática de los documentos digitales, ha quedado demostrado que eso no es posible, y que la fiabilidad, autenticidad, etc. de un documento de archivo digital se establecen analizando:

1) Los procedimientos de producción del documento,

2) La calidad y acuciosidad de la cadena de preservación del documento de archivo, y

3) La confianza en el custodio, dada por su competencia, desempeño y reputación.

La preservación es un proceso deliberado

Por lo mismo, nótese que la preservación de los documentos de archivo digitales es un proceso continuo que inicia desde el primer momento de su producción, y continúa ininterrumpidamente.

Garantizar la autenticidad de documentos de archivo digitales requiere de la acción deliberada y la intervención de instancias confiables con responsabilidad de rendición de cuentas, así como de un adecuado marco de referencia de políticas, procedimientos y tecnologías.

La preservación de documentos de archivo digitales implica que:

1) Existe una serie de requerimientos que deben implantarse desde el principio en todo sistema de gestión archivística dedicados a producir documentos de archivo digitales fiables y exactos y a mantener documentos de archivo auténticos;

2) En realidad NO preservamos documentos de archivo digitales; pero sí podemos preservar la capacidad de reproducirlos o recrearlos una y otra vez; cuando salvamos un documento de archivo lo separamos en sus componentes digitales y cuando lo recuperamos y lo reconstruimos adecuadamente lo reproducimos. ***(Duranti y Thibodeau , 2005*****)**

La preservación de documentos de archivo digitales implica que:

3) En el documento de archivo digital el contenido, la estructura y la forma no están ya inextricablemente entrelazados.

4) La entidad almacenada es distinta de su manifestación; no obstante, la normatividad exige cada vez más que la presentación digital sea considerada tan válida como su presentación documental tradicional.

5) Tarde o temprano debemos hacer una inferencia de autenticidad del objeto-documento de archivo que ha sido compuesto, almacenado, reproducido y transformado. Sin elementos es muy difícil, si no imposible, hacer esa valoración

La declaración de autenticidad se basa en:

1) Los procedimientos de producción del documento.

"El conjunto de reglas y procedimientos que controlan el proceso de formación y producción de documentos de archivo y su información, así como las aplicaciones informáticas, herramientas y mecanismos utilizados para implementar esas reglas y asegurar la calidad".

(Glosario InterPARES)

La declaración de autenticidad se basa en:

2) El seguimiento escrupuloso de la "Cadena de Preservación" (la secuencia de controles que se extiende sobre todo el ciclo de vida de los documentos de archivo para asegurar su identidad e integridad a lo largo del tiempo*.

Esto implica que el documento de archivo siempre ha estado bajo un *'custodio de confianza'* y cuenta con todos sus metadatos de autenticación (identidad e integridad).

Por lo mismo, se subraya que la preservación de documentos de archivo digitales es un proceso continuo que inicia desde el primer momento de su producción y continúa ininterrumpidamente. ***Glosario InterPARES.***

Metadatos de autenticación:

Contienen la información de los atributos extraídos del documento de archivo digital que conllevan su identidad e integridad y por tanto su autenticidad:

Los metadatos que conllevan los requisitos de identidad son: ***nombre de las personas que intervienen en el documento de archivo (autor, escritor, originador, destinatario); nombre de la acción o materia: fechas del documento de archivo (cronológica, de recepción, de archivo, de transmisión); el vínculo archivístico (código de clasificación, identificador del expediente); y la indicación de anexos.***

"Requirements for assessing and maintaining the authenticity of electronic records". InterPARES (2002).

Metadatos de autenticación:

Contienen la información de los atributos extraídos del documento de archivo digital que conllevan su identidad e integridad y por tanto su autenticidad:

Los metadatos que conllevan los requisitos de integridad son: ***nombre de la oficina operaria, nombre de la oficina de responsabilidad primaria, auditoría del tipo de anotaciones hechas al documento de archivo y control de cambios, los privilegios de acceso y el registro de todas de modificaciones técnicas realizadas al documento (refresco, migración, etc.).***

"Requirements for assessing and maintaining the authenticity of electronic records". InterPARES (2002).

Metadatos de autenticación:

Existen además los metadatos que se extraen de los contextos* y se encuentran como externos al documento de archivo y se construyen por serie o fondo. Por ejemplo: ***leyes y reglamentos que dieron origen a la producción del documento; organigramas de la institución; características del sistema informático; ubicación del servidor si el fondo se hospeda en la nube; los procedimientos que garantizan la integridad e identidad de los documentos de archivo de un fondo a través de la obsolescencia tecnológica, entre otros.***

**** Contextos Jurídico-administrativo, legal, de procedencia, procedimental y tecnológico)***

"Requirements for assessing and maintaining the authenticity of electronic records". InterPARES (2002).

La declaración de autenticidad se basa en:

3) La confianza en el custodio, dada por su competencia, desempeño, solvencia y reputación. ***La organización custodio requiere crear una confianza, la cual es la seguridad de una expectativa de acción y conducta que el público tiene en su organización; esa confianza está basada en:***

- ***Desempeño, el cual es la relación entre las acciones presentes del custodio y la conducta requerida para cumplir con sus responsabilidades cotidianas especificadas por el público;***
- ***Competencia, la cual consiste en la posesión de conocimientos, habilidades, talentos y características necesarias para poder realizar una tarea de cierto nivel.***
- ***Solvencia, la cual es la seguridad de una expectativa de acción y conducta que el confiante tiene en el custodio; y***
- ***Reputación, la cual consiste en la evaluación de las acciones y conductas pasadas de esa organización custodio;***

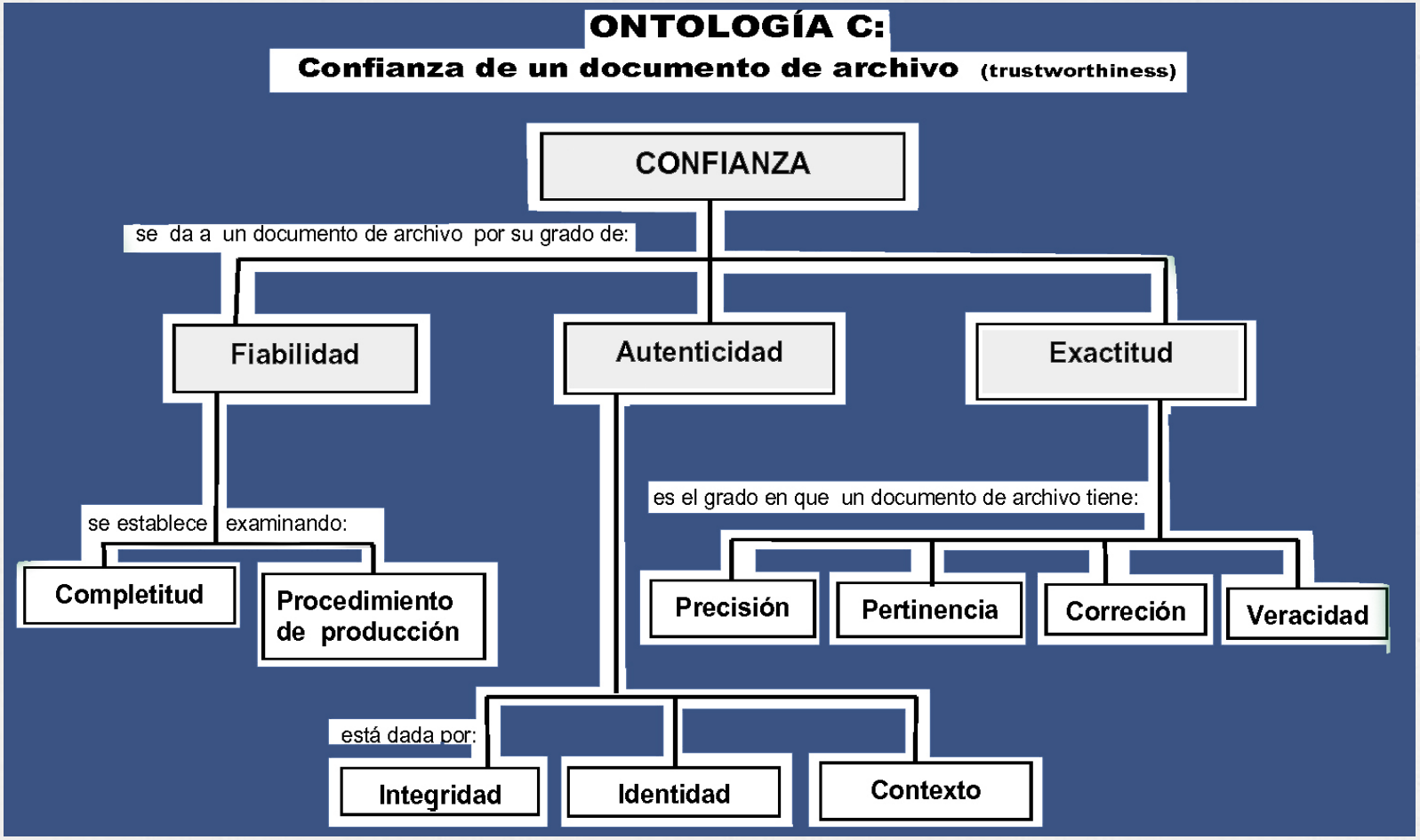
Sztompka, Piotr. (1999) "Trust". Cambridge : Cambridge University Press. ISBN: 0521-59850-8.

Autenticidad

Por tanto, en el medio de los documentos de archivo digitales la autenticidad documental es *una inferencia basada en evidencia fundada (procedimientos, metadatos de autenticidad, cadena de preservación) así como en la confianza en el desempeño y competencia del custodio de la información, de acuerdo con su solvencia y reputación*.

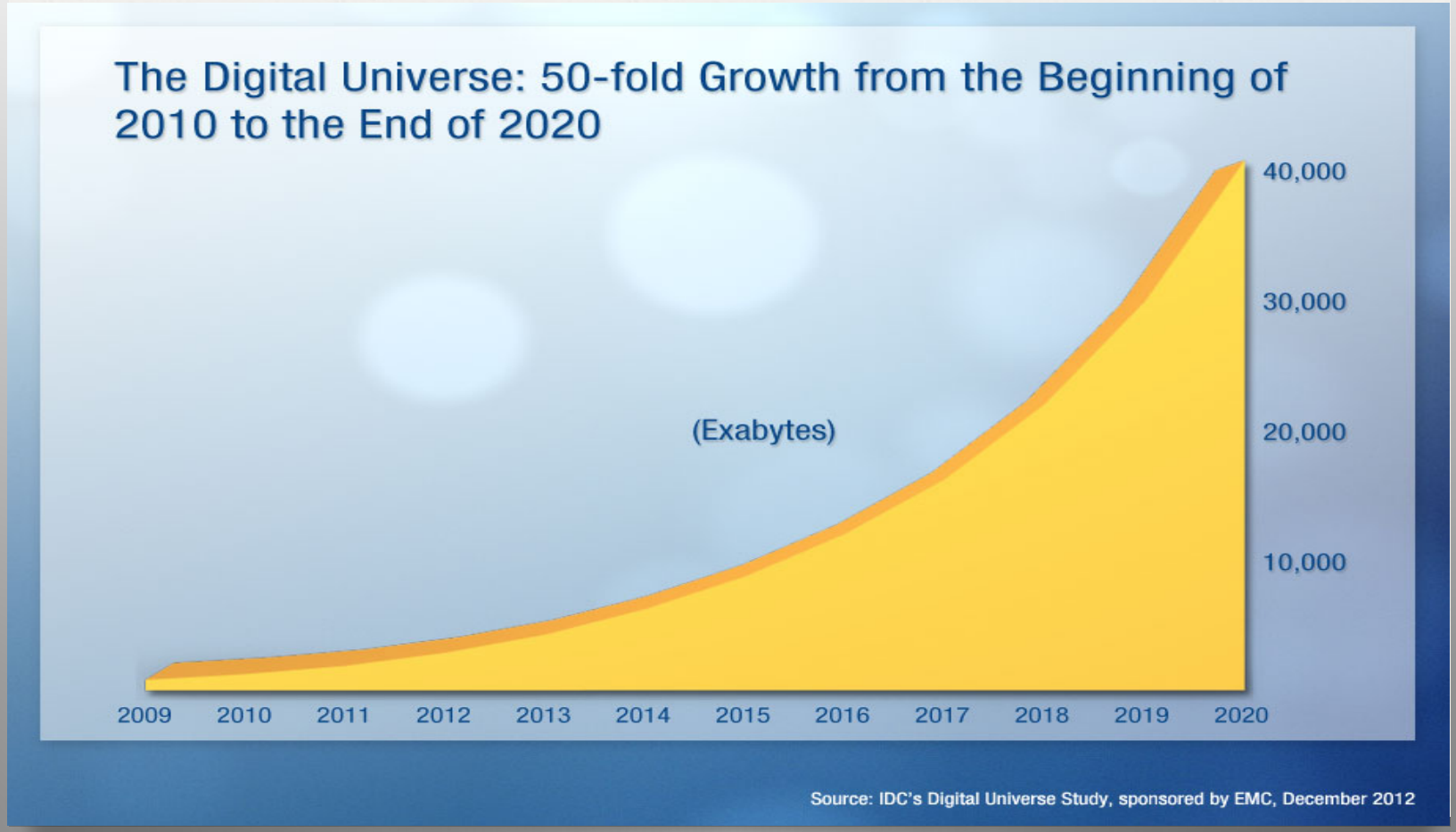
Garantizar la autenticidad de documentos de archivo digitales requiere de la acción deliberada y consistente de instancias confiables con capacidades técnicas y responsabilidad de rendición de cuentas, así como de un adecuado marco de referencia de políticas, procedimientos y tecnología.

Confianza de un documento de archivo (Interpares, 2004)



Nuevos retos:

El crecimiento exponencial de la información digital a nivel mundial, en la cual los archivos digitales se encuentran cada vez más inmersos.



Nuevos retos

La fuerte tendencia mundial experimentada en años recientes por parte de los gobiernos de una gran mayoría de países hacia la transparencia, la rendición de cuentas y la participación ciudadana, con miras hacia los conceptos de "gobierno abierto*" - *open-government*, en un futuro cercano, y en los que los archivos digitales han jugado y jugarán un papel cada vez más preponderante y su demanda y uso crecerá veriginosamente.

El advenimiento y fuerte presencia de los servicios de Cómputo en "*la Nube*" crea un nuevo ambiente en el que -de acuerdo con el estado del arte actual- la organización usuaria no tiene control sobre los servidores y/o sistemas rentados por ella. Las reglas de control y acceso para establecer las premisas de autenticidad, fiabilidad, etc., se ven totalmente trastornadas y pueden quedar seriamente inutilizadas.

*** Lathrop, Daniel; Ruma, Laurel, eds.** 2010. *"Open Government: Transparency, Collaboration and Participation in Practice"*. O'Reilly Media. ISBN: 978-0-596-80435-0.

Nuevos retos

Con las teorías, conceptos, modelos y estudios analizados se establecieron reglas y recomendaciones que han permitido a los responsables de archivos en organizaciones producir y mantener colecciones de documentos de archivo cuya fiabilidad y autenticidad puede ser establecida y reconocida de acuerdo con convenciones internacionales. Pero todo ello se ha basado en la premisa que la organización ha podido tener absoluto control tanto de los procedimientos internos de gestión como del servidor de cómputo que guarda los archivos de la organización.

El advenimiento y fuerte presencia de los servicios de Cómputo en "*la Nube*" crea un nuevo ambiente en el que -de acuerdo con el estado del arte actual- la organización usuaria no tiene control sobre los servidores y/o sistemas rentados por ella. Las reglas de control y acceso para establecer las premisas de autenticidad, fiabilidad, etc., se ven totalmente trastornadas y pueden quedar seriamente inutilizadas.

Nuevos retos

Crear confianza, no solo en los documentos; también en las organizaciones que los manejan y custodian.

Nuevos retos:

El público espera en que las organizaciones que guardan archivos digitales (sistema tributario, sistema educativo, registro civil, compañías de luz, teléfono, bancos, etc.), conserven y mantengan adecuadamente esos datos digitales, documentos de archivo y archivos históricos a ellos encomendados. Aunque en realidad, no sepamos dónde residen esos documentos, ni si están siendo seriamente manejados, ni por cuánto tiempo estarán disponibles.....

- Las organizaciones ya se están preocupando por una responsabilidad que posiblemente no pensaron que estaban asumiendo, al tiempo que están amasando enormes volúmenes de datos que usan para proporcionar una serie de servicios, tanto públicos como privados.

-Las personas ya se están preocupando por el manejo que las organizaciones hacen de esa información, creándose un problema de confianza entre ellos y las organizaciones depositarias, y cuyo balance es necesario reponer.

Nuevos retos:

Las organizaciones custodio, como representantes de un gobierno abierto y transparente, requieren solvencia; es decir, crear una confianza de su público en ellas, la cual es la seguridad de una expectativa de acción y conducta que se tiene en la organización, creada y mantenida por su competencia, desempeño y reputación.

solvencia = trustworthiness

Al final, los retos son los mismos:

1) Preservar los documentos de archivo digitales a pesar de los cambios, la obsolescencia tecnológica y la *nube*.

2) Preservarlos auténticos, íntegros y confiables (en organizaciones confiables)

Las reglas cambian, y debemos adaptarnos para lograrlo.

Juan Voutssás

voutssas@unam.mx

Bibliografía:

-**Duranti, Luciana, and Thibodeau, Kenneth.** 2005. *"The concept of record in interactive, experiential and dynamic environments: The view of InterPARES"*. In: "Archival Science". Springer Netherlands. ISSN:1389-0166 (Print) 1573-7519 (Online). Vol. 5 Nums. 2-4. December 2005. DOI 10.1007/BF02660804. pp.13-68.

Glosario Interpartes de Preservación Archivística Digital. 2014. UNAM : Instituto de Investigacones Bibliotecológicas y dela Información. Disponible en: http://iibi.unam.mx/archivistica/glosario_preservacion_archivistica_digital_v4.0.pdf

InterPARES - The International Research on Permanent Authentic Records in Electronic Systems. 2002. *"Requirements for assessing and maintaining the authenticity of electronic records"* InterPARES Authenticity Task Force. Appendix 2 from book "T*he Long Term Preservation of Authentic Electronic Records"*. Disponible en: http://www.interpares.org/book/interpares_book_k_app02.pdf

InterPARES – *"Guía del Productor de Documentos de Archivo".* 2006. Disponible en: http://iibi.unam.mx/archivistica/Guia_del_Productor/Guia_del_Productor.html

InterPARES – *"Guía del Preservador de Documentos de Archivo".* 2006. Disponible en: http://iibi.unam.mx/archivistica/Guia_del_Preservador/Guia_del_Preservador.html

-**Mell, Peter and Grance, Timothy.** 2011. *"The NIST Definition of Cloud Computing : Recommendations of the National Institute of Standards and Technology"*. NIST Special Publication 800-145 . Sept. 2011. Disponible en: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

-**Delgado, Alejandro. 2013.** *"La Nube"*. En: "Legajos" Boletín del Archivo General de la Nación. México, AGN, 7ª época, año 4, No. 16. 2013. pp. 107-122. ISSN: 0185-1926.

-**Voutssás M., Juan.** 2013. *"Documentos de Archivo en la Nube : Evolución y Problemática".* En: "Legajos" Boletín del Archivo General de la Nación. México, AGN, 7ª época, año 4, No. 17. 2013. Disponible en: http://iibi.unam.mx/~voutssasmt/documentos/legajos_17_nube_corto.pdflegajos17_nube_corto.pdf

-**Voutssás M., Juan.** 2012. *"La Autenticidad en Documentos de Archivo Digitales : Una Ontología"*. En: "Legajos" Boletín del Archivo General de la Nación. México, AGN, 7ª época, año 3, No. 12. 2012. pp. 55-72. ISSN: 0185-1926. Disponible en: http://iibi.unam.mx/archivistica